Technical Proposal US 84-10/9

Data Protection and Privacy: Comparative Policies

A Report to the Government Information Technology Project

Office of Technology Assessment, U. S. Congress

David H. Flaherty
Professor of History and Law

January 8, 1985

The Privacy Project
University of Western Ontario
London, Canada N6A 5C2
Telephone: (519) 679-2800

This contractor document was prepared by an outside contractor as an input to an ongoing OTA assessment. It does not necessarily reflect the analytical findings of OTA, the Advisory Panel, or the Technology Assessment Board.

J952-45

Table of Contents

Executive Summary iii

1. Introduction 1

2. Implementation of Data Protection in National Systems 6
    - 2.1 Federal Republic of Germany 6
    - 2.2 Sweden 14
    - 2.3 France 18
    - 2.4 United Kingdom 24
    - 2.5 Canada 27
    - 2.6 Australia 32
    - 2.7 Japan 35

3. Record Linkages: Computer Matching and Computer Profiling 44
    - 3.1 Canada 46
    - 3.2 Sweden 49
    - 3.3 France 52
    - 3.4 United Kingdom 53
    - 3.5 Federal Republic of Germany 54
    - 3.6 Australia 61

4. Personal Identification Numbers 66
    - 4.1 Sweden 67
    - 4.2 Federal Republic of Germany 69
    - 4.3 France 70

5. Machine-Readable Identity Cards and "Smart" Cards 74

  - 5.1 Federal Republic of Germany 74
  - 5.2 Canada 76
  - 5.3 Sweden 76
  - 5.4 France 77

6. Conclusions 82

Research Note 88

Appendices:
1. The West German Act on Protection against the Misuse of Personal Data in Data Processing of January 27, 1977.
2. The Swedish Data Act, as amended with effect from July 1, 1982
3. The French Act 78-17 of January 6, 1978 on Informatics, Data Banks, and Freedoms.
4. The United Kingdom's Data Protection Act 1984.
5. The Canadian Federal Privacy Act of 1982.

Executive Summary

The primary purpose of this research report is to produce information and ideas that are relevant to a study of Federal Government Information Technology being carried out by the Office of Technology Assessment of the U.S. Congress. The emphasis is on issues of direct relevance to the OTA study of United States federal government personal information practices. This includes available data on such pressing concerns as computer matching, computer profiling, and the use of the Personal Identification Number.

The most important single issue treated in this research report is the process of implementation of data protection in the relevant countries, since, in the author's judgment, implementation is the single greatest deficiency in American federal data protection policies and practices.

The nature and length of this report were established by the terms of the contract proposal from the Office of Technology Assessment of the U.S. Congress. It is based for the most part on research conducted by the author since 1981 for a research project entitled "Data Protection Compared: an International Perspective," which has involved an intensive study of how data protection agencies and data protection officials have been working in practice for the public sector at the national level in six countries: Sweden, the Federal Republic of Germany, France, the United Kingdom (law only; no experience), and Canada.

A very important distinction, adopted throughout this report, is the difference between privacy protection and data protection. As an American reader is especially aware, the legal right to privacy can be used to refer to an enormously wide range of issues from the right to engage in certain types of sexual practices to the use of various kinds of surveillance devices. What is being discussed in this report is that aspect of the protection of personal privacy that concerns the collection and use of personal data; in a sense, this subset of the privacy field can most usefully be referred to as data protection, the term that in fact will be used throughout this report.

Chapter two on the implementation of data protection in national systems is to present basic information about the systems of data protection for the public sector that exist in a variety of foreign countries. The emphasis is on the general outlines of each system, especially the process of implementation, since the laws share a common core of principles traditionally associated with fair information practices, and the details of each system frequently reflect general differences in constitutional and administrative practices among countries. The emphasis is on the fact that the European (and Canadian) Data Protection Commissioners or data protection agencies are essentially specialists in the articulation of privacy and data protection interests with respect to information handling practices.

Chapters two to five discuss certain specific problems of data protection, because they are of particular interest to the Office of Technology Assessment's study of federal information technology and because they are issues that concern data protectors in all of the countries that have data protection laws. Chapter three looks at a group of associated issues that can be roughly described as record linkages, computer matching, and computer profiling. The critical term is in fact record linkages, because one is in fact focusing on the use of computers to integrate discrete items of personal information from separate personal data systems. Despite the attention already paid to the problem of computer matching in the United States, it must be kept in mind that such types of record linkages are automatically caught up in the normal net of data protection activities in European countries and in Canada. In general terms, the European data protection laws require advice or consent for government record linkages.

Chapter four deals with Personal Identification Numbers (PINs), which are a generic reference to a whole series of numerical identifiers. An ideal PIN is a unique number assigned at birth that follows a person through life and is widely used in society for all administrative purposes. Few Western countries have truly unique numbers that are in common use for each citizen. Of the countries treated in detail in this research report, only Sweden has a PIN system that is mature and fully developed. The other countries have numbering systems with varying kinds of problems, comparable to the unreliability of the Social Security Number in the U. S. as a unique personal identifier. It is somewhat surprising that data protection laws do not specifically address the issue of PINs or other numbering schemes in use in the society; as a general rule the laws are silent on the problem, in part because most countries do not have single unique personal identifiers. The main point about PINs, whether unique identifiers or not, is that they are subject to strong resistance in Western Europe and North America, because persons believe that they threaten the very roots of personal privacy and individuality.

Chapter five treats machine-readable identity cards and other forms of so-called "smart" cards. The identity cards in question essentially involve a traditional plastic credit card impregnated with selected amounts of personal data, which a machine can scan very quickly in order to validate a transaction such as crossing a national boundary. The latter is the most commonly discussed application of the cards at present, but what is inevitable is that new applications will be invented as fast as machine-readable cards can be dispensed; thus they do pose a significant challenge to the individual interests that data protectors are trying to protect through the application of their general laws in specialized laws or regulations.

The primary conclusion of this report, and of the author's ongoing research on "Data Protection in Comparative Perspective," is that the system of data protection in place for the public sector at the federal level in the United States is sorely lacking one key ingredient, and that is an effective oversight mechanism to ensure that the Privacy Act of 1974 is implemented in an appropriate fashion. The argument that a data protection agency (or agent) is essential for successful implementation of data protection laws is not an assumption on the author's part but a personal judgment. It is a major conclusion of an international research project on data protection, begun in 1981, involving considerable interviewing and empirical research in six countries that are the primary targets of research, plus some direct exposure to the situation in Denmark and Norway.

The lack of a federal data Protection Commission in the United States is a source of concern to foreign data protectors, since they believe that an agent or agency is an essential component of a data protection system, a perspective reinforced by the fact that all other national laws include an oversight mechanism. Moreover, the Europeans have no comparable agency in the United States to deal with, especially on the sensitive subject of transborder data flows of personal information.

The author's general approach is to identify certain problems of the data protection movement, while being fundamentally committed to its general goals. No one should be led to believe that a Data Protection Commission in the United States would be a universal panacea and/or always succeed in resolving conflicts over values in the direction of promoting privacy. One of the lessons of the material presented in chapters 2 to 5 is that data protection agencies are only one player on the political and legislative scene; nevertheless, it seems essential that this player be on the field when interests affecting privacy are under discussion. Protecting privacy begins with problems of definition and moves inexorably towards difficulties in balancing competing values in an intelligent and rational fashion. The issues arise on and item by item basis, as the discussion in this report suggests.

The central function of a data protection agency is to seek to resolve specific data protection problems. The experience to date suggests that these new mechanism are both qualified and competent to accomplish these tasks. The irony is that this same impulse leads to the accusation that data protectors may in fact function as legitimators of new information technology and new practices, such as record linkages. In the author's judgment, it is in the best interests of any society to have in place a mechanism that can review, modify, and ultimately accept, or at least tolerate, such innovative activities.

1. Introduction

The primary purpose of this research report is to produce information and ideas that are relevant to a study of Federal Government Information Technology being carried out by the Office of Technology Assessment of the U.S. Congress. Although there is some presentation of background material in order to make comprehensible the system of data protection in place in the countries covered in this report, the emphasis is on issues of direct relevance to the OTA study of United States federal government personal information practices. This includes available data on such pressing concerns as computer matching, computer profiling, and the use of the Personal Identification Number. Although these particular topics are the primary focus of the materials presented below, it should be recognized in advance that the secondary literature is very thin on some of these specialized questions. It has been possible, in certain cases, to obtain additional information on specific issues by direct contact with data protectors in Canada and Western Europe. Because of lack of data, certain other informational privacy issues are not discussed, such as the privacy implications of electronic mail. But because of the systems of data protection in place in Canada and Western Europe, such new issues are automatically on the agenda of data protectors.

The most important single issue treated in this research report is the process of implementation of data protection in the relevant countries, since, in my judgment, implementation is the single greatest deficiency in American federal privacy policies and practices.[1] An analysis and summary of my views on the strengths and weaknesses of the data protection movement in Western Europe can be found in a recent essay.[2] The ideas in this essay, which to a certain extent are elaborated on and reformulated in chapter 5 of this research report, will be important for OTA to grapple with in designing and recommending an appropriate and effective federal system of implementation for data protection in the United States.

This research report to OTA emphasizes the personal information practices at the national level of the following countries, which have experience in many of the areas of interest to OTA's study of Federal Government Information Technology: Sweden, the Federal Republic of Germany, France, the United Kingdom (law only; no experience), and Canada. Where relevant to the analysis of specific issues, selective references are made to the OECD Guidelines for the Protection of the Personal Information and the Council of Europe's Convention on the same subject, which is about to acquire the force of law.

A very important distinction, adopted throughout this report, is the difference between privacy protection and data protection. As an American reader is especially aware, the legal right to privacy can be used to refer to an enormously wide range of issues from the right to engage in certain types of sexual practices to the use of various kinds of surveillance devices.[3] What is being discussed in this report is that aspect of the protection of personal privacy that concerns the collection and use of personal data; in a sense, this subset of the privacy field can most usefully be referred to as data protection, the term that in fact will be used throughout this report. Relying on the term "data protection" also introduces some intellectual rigour into what is otherwise a very fuzzy concept of "privacy." Although specialists can make the necessary distinctions between various aspects of concern for personal privacy, use of the term "privacy protection" with the general public seems to involve much too eclectic a range of issues and to confuse rather than clarify the subject. The British are to be congratulated (among English-speaking countries) for calling their new statute a "Data Protection Act;" in fact, the word privacy does not appear anywhere in the law.

Readers will find that documentation and footnoting have been kept to a minimum in what follows, except for essential items. This reflects the fact that the author of this report has just published Privacy and Data Protection: An International Bibliography.[4] Complete, annotated entries for the abundant literature on privacy and data protection published through the spring of 1983 will be found in this volume. A few more recent publications are included in the footnotes to this report, where relevant.

The nature and length of this report were established by the terms of the contract proposal from the Office of Technology Assessment of the U.S. Congress. Funding was not available for additional interview research, although this report includes information from interviews conducted by the author in Europe and Canada in December 1984. Thus this report is based for the most part on research conducted since 1981 for a research project entitled "Data Protection Compared: an international perspective." A book by the same title is in the final stages of completion. This project has involved an intensive study of how data protection agencies and data protection officials have been working in practice for the public sector in six countries, including Canada, the United States, Sweden, the Federal Republic of Germany, France, and the United Kingdom. Hundreds of interviews have been conducted in each country since 1981, with particular emphasis on the actual work of data protection officials. Thus this report for OTA in fact represents the tip of the iceberg of research and writing already completed on a scale beyond the scope of this particular report. Summary judgments reported here are drawn from the experience of research and writing for the larger Privacy Project.

For their assistance in preparing this report and for general

assistance in the Privacy Project, I would like to thank my research assistants, Peter J. Harte and Terence J. Donohue, and my secretaries, Lizbeth Carruthers and Penelope Lister. I owe a particular debt of gratitude to the hundreds of government officials, academics, and private consultants who have generously allowed me to interview them in connection with my major research project. It is also essential to acknowledge the generous financial support that the Privacy Project has received since 1981 from the Ford Foundation, the Social Sciences and Humanities Research Council of Canada, and the Academic Development Fund of the University of Western Ontario.

David H. Flaherty

Notes-Introduction

1. For an indication of my views, see David H. Flaherty, "The Need for an American Privacy Protection Commission," Government Information Quarterly, I, No. 3 (1984), 235-58. Although this essay primarily reviews the domestic rationale in the US for such a Commission, the comparative comments on European and American data protection at pages 249-53 are directly relevant to this particular research report for OTA.

2. Flaherty, "Limiting Governmental Surveillance and Promoting Bureaucratic Accountability: The Role of Data Protection Agencies in Western Societies,"An unpublished essay delivered at the 1984 Annual Meeting of the American Political Science Association, Washington, D.C. August 31, 1984.

3. See, for example, the wide-ranging discussion of recent privacy cases by Ronald Dworkin in The New York Review of Books, November 8, 1984, pp. 27-31.

4. David H. Flaherty, editor, Privacy and Data Protection: An International Bibliography (Mansell, London, UK, 1984; and Knowledge Industry Publications Inc., White Plains, NY, 1984)

2. Implementation of Data Protection in National Systems

The purpose of this chapter is to present basic information about the systems of data protection for the public sector that exist in a variety of foreign countries. The emphasis will be on the general outlines of each system, especially the process of implementation, since the laws share a common core of principles traditionally associated with fair information practices, and the details of each system frequently reflect general differences in constitutional and administrative practices among countries.

2.1 The Federal Republic of Germany:

The European (and Canadian) Data Protection Commissioners or data protection agencies are essentially specialists in the articulation of privacy and data protection interests in their respective spheres. The West German system of data protection is the most relevant to the United States, because it also has a large population and a federal system; it illustrates one model of how a Data Protection Commission in the United States could function.

The Federal Data Protection Act in West Germany became law on January 27, 1977.[1] Its detailed principles for data protection in the public sector are directly comparable to the system of fair information practices previously incorporated in the American Privacy Act of 1974. The detailed differences are not important for present purposes. What is significant is that West Germany has a coordinated system of implementation in place for the federal and state data protection acts. Independent officials responsible for data protection exist in all of the eleven Länder or states. In fact, the Land of Hesse passed the first general data protection law in 1970 and has had a Data Protection Commissioner since that time. Although each federal and state data protection office has separate statutory jurisdiction over the public sector, the respective officials meet regularly to shape common positions on various issues.

The West German and American data protection laws are comparable in that the heads of federal government agencies have primary responsibility to ensure that the laws are implemented. The basic obligation to see that the statute is enforced rests with the head of the particular government Ministry. West Germany is a law-driven society, meaning that almost every information-collection activity of government is regulated by a particular statute, and every civil servant acknowledges a direct legal responsibility to implement general and specific data protection measures. This system works well in West Germany because many of the civil servants are trained in law.

The American and West German federal data protection statutes diverge significantly with the appointment of a Federal Data Protection Commissioner (and state counterparts) in the latter country. It is important to realize that this position was added to the draft legislation at the insistence of the West German legislature; the original government bill omitted such an official. The opposite happened in the United States, where House-Senate conferees dropped the idea of a Privacy Protection Commission from the Senate version of the Privacy Act, because of the fear of a veto by President Gerald Ford.

The Federal Data Protection Commissioner serves a five-year term and is "independent in the performance of his duties and subject to the law only."[2] The degree of statutory independence from the government is a particularly important characteristic of all such offices, in West Germany and elsewhere. The duties of the Data Protection Commissioner are to ensure that the Data Protection Act are implemented in the federal public sector. He makes recommendations for the improvement of data protection and may give advice to the federal government and individual ministers.[3] He is required to present an annual detailed activity report to the legislature, which is one of the main ways of assessing the state of progress with respect to the implementation of data protection.[4] At present, aspects of this annual report are discussed by as many as nine committees of the Bundestag. When Dr. R. Baumann, the current Commissioner, gave his views of an experimental on-line motor vehicle data base, known as ZEVIS, the Committee of the Interior ordered a halt to the system until a special law could be framed to regulate it from a data protection point of view.

The Federal Data Protection Commissioner has advisory powers only. If he discovers "infringements against the provisions of this [1977] Act, against other data protection regulations, or other irregularities in the processing of personal data," he can submit a complaint to the relevant authority.[5] To this point in time, such advice has been taken seriously by federal agencies, including the national security agencies and the federal police. In essence, it has not been politically viable for the heads of federal agencies to ignore the advice of the Data Protection Commissioner, which is normally given privately in the first instance and as part of a process of negotiation over competing interests in the use of information. The office only issues critical public statements when fundamental differences of opinion occur, or serious breaches of the data protection law have been found during an audit or inspection of a particular information system. In his fifth and last annual report. Professor Bull pointed out that of thirty-one inspections carried out at government agencies in 1982, only seven resulted in the presentation of formal objections to current practices, primarily pertaining to issues of security and length of data storage. The Federal Data Protection Commissioner's office also receives communications and complaints from individuals, which identify possible problems.[6]

The office of the Federal Data Protection Commissioner (BfD) has a staff of about thirty-five persons, at least half of whom are professionals (mainly persons with academic training in law). Although formal opinions and recommendations are made in the name of the Data Protection Commissioner, the staff function in a collegial fashion by means of regular weekly meetings. They specialize in various types of federal information systems, in recognition of the important fact that the application of data protection is very complicated, because principles need to be adapted to the particular characteristics of each personal-information system.

A primary goal of the West German data protection offices is to ensure that specialized data protection measures are incorporated in the detailed laws governing each type of information-handling activity in the public sector. The national data protection law establishes the general regime, which then is shaped and reshaped for particular applications in specialized legislation for various types of information systems. This particular activity is a central goal of data protection in every country; it requires the consistent application of accumulated expertise on behalf of privacy interests. In this sense, the American and West German federal systems of data protection seem quite similar. The Privacy Act of 1974 is the general law; an example of its specific refinement is Section 631 (on protection of subscriber privacy) in the federal Cable Communications Policy Act of 1984. But the U.S. government does not benefit in such matters from the advisory services of a permanent independent office comparable to the West German Data Protection Commissioners.

The first six years of the implementation of data protection in West Germany, especially at the federal level, are generally thought to have been very successful. In particular, the 1977 law has had signficant life breathed into it through effective efforts at implementation. The general public is aware, for the most part, that data protection officials are in place and at work, especially since the 1983 census controversy before the Federal Constitutional Court created such an uproar. With Professor Hans Peter Bull of the University of Hamburg as the first federal Data Protection Commissioner from 1978 to 1983, the data protectors learned a great deal about the real state of data processing and data communication and also discovered that certain anxieties of the general public about widespread record linkages were unfounded. The office emphasized audit and inspection activities to learn how personal information flows into and through every type of data system in the federal government and how the principles of the data protection legislation were being followed in practice. Its staff became consultants to government agencies on the efficient movement of personal data, illustrating its cooperative approach to implementation. Thus the data protection initiative coincided with other significant societal interests, such as the reduction of costs of data handling and the promotion of efficiency in the transmission of personal information within scattered units of a federal ministry, such as the federal criminal police. Data protectors in Western Europe are not hostile to the promotion of efficient and less costly government, so long as the privacy interests of the citizenry are reasonably protected in the process.

Even though the Office of the Federal Data Protection Commissioner does not have the direct power to order a particular thing to be done or not to be done, this has not hindered the successful conduct of data protection to date. The Commissioner has simply inserted and asserted his views on the proper protection of privacy interests in the political process of decision-making. However, a few West German data protectors are beginning to talk about the need for a limited use of "a licensing system" for certain types of sensitive systems of personal information, but this minority view is not reflected in the emerging proposals for minor amendments to the federal law. To the extent that the "licensing" proposal is emerging, it simply reflects the frustrations of a small number of data protectors faced with a series of large tasks with only advisory powers to rely on. The latest annual report of the BfD for 1983 does not discuss licensing at all.

Despite the inevitable conflicts with certain public administrations, especially those in the early years that did not want another watchdog over their activities (a standard bureaucratic response in every country), the Federal Data Protection Office has done its work without any major breakdown in its relationship with the subjects of regulation. Initial resistance was always overcome through a process of friendly persuasion. In many ways this success is surprising, given the contentious character of some of the matters in dispute in the police and security fields in particular, but it is a description of working reality. The annual activity reports of the Office are full of specific illustrations of progress achieved, even if many problems continue to exist. For example, the staff of the federal office regularly questioned the need for collection, retention, or transmission of certain items of personal data. In many ways the various data protectors at the federal and state levels have successfully engaged in a very active program of consciousness-raising in the public administration; the general public, the government, and the legislature have generally supported their efforts.

Some Special West German Issues

The conservative Minister of the Interior decided not to reappoint Prof. Bull, a Social Democrat, after the end of his five-year term as Federal Data

Protection Commissioner, allegedly because Bull had been too tough with police and national security agencies. He appointed a career civil servant, Dr. R. Baumann, to succeed him. This decision could have very negative implications for the independence of the Data Protection Commissioner, since many persons holding such a sensitive position would not enjoy the luxury of being able to return to a university professorship, if they lost their job at the end of a five-year term. Effective data protection requires occasional confrontations with the government, which only a truly independent official will be able to risk. There were similar risks that the appointment of a successor from within the Ministry of the Interior might have weakened the process of data protection, since the incumbent would have less inclination than an outsider to challenge government departments on specific points.

The evidence of the first year-and-a-half in office of Dr. Baumann suggests that the work of the BfD is continuing along its established lines. Baumann has the insider's advantage of knowing a significant number of high level officials, with whom he can settle incipient problems on an immediate and informal basis. Although Dr. Baumann planned to use the media less frequently than Prof. Bull, the enormous publicity achieved by data protection in West Germany in 1983, because of the census controversy, has meant that Dr. Baumann (and his state colleagues) have in fact been very much in the public eye. Although the Minister of the Interior may have expected in the spring of 1983 that data protection would become less visible, such has not been the case.

The Federal Constitutional Court postponed the West German census of population in the spring of 1983 on grounds of potential invasion of privacy, despite the passage of the census law by a unanimous legislature in 1982 and the general acceptance by data protection specialists of the census law.

Continued public anxieties about such a relatively innocuous activity as the taking of a census are a reminder of how much people continue to worry about the erosion of their personal privacy in this era of information technology.

On December 15, 1983 the Federal Constitutional Court in Karlsruhe ruled unanimously in the census case that West Germans have a constitutional right to self-determination about information about themselves. Although this right is not absolute in the face of competing societal values, information use, the court ruled, has to occur on the basis of established laws. This requires, in essence, a law to regulate each activity involving the collection and use of personal data. The court's positive ruling on the census is only a minor part of this momentous decision of Judge Benda and his eight colleagues. It is arguable that they have created a constitutional right to data protection in response to what Prof. Simitis, the Hesse Data Protection Commissioner, has described as the first mass movement for data protection in West German history during the census controversy. The population rose up against the proposed census in the spring of 1983 because of its fears about the use of computers in data processing. The Federal Constitutional Court has in effect given constitutional status as well to data protection agencies. West German data protectors are now intensely preoccupied with interpretation of the implications of this decision for their work. Their activities have been given strong reinforcement in the public sector by the court's decision, which has also routed the (few) critics and opponents of data protection activities.

One current concern of the Federal Data Protection Office is the burden of work on a small staff. The basic attention of the office goes from one major problem area, such as the census, to another. Every staff member has a heavy load of consulting, advising, and reporting on current issues. The risk of such crisis management is neglect of the function of auditing and inspecting government data bases on a systematic basis.

2.2 Sweden:

The Swedish Data Act of 1973, the first national law of its type in any country, has now been fully and successfully in effect for a decade. It also continues to have a great influence on the development of national data protection statutes in other Western countries. France and the United Kingdom have both adopted data protection regimes influenced by the Swedish model of having a Data Inspection Board (DIB) to license all automated personal information systems in both the public and private sectors.

The goal of the Data Act is to prevent "undue encroachment on the privacy of registered persons." In judging this risk, the statute instructs the DIB to pay special attention "to the nature and quantity of the personal data to be recorded in the file, to how and from whom the data are to be collected, and to the attitude to the file held by, or which may be assumed to be held by, the persons who may be registered. "It is unlawful to start or maintain a personal data base (Swedes use the terms "personal file" or "register") in machine-readable form without applying for and obtaining a license from, and in certain sensitive cases the permission of, the DIB, unless the Cabinet or Riksdag (legislature) creates it.[8] The original statute mandated DIB licensing in advance, but a more permissive and somewhat less bureaucratic system, focusing more on sensitive uses of personal data, was introduced in the 1982 revision. Continental European data protection laws generally define certain types of personal data, such as information on criminality, political views, religious beliefs, or psychiatric care, as more sensitive than others. The 1982 Swedish law is especially detailed on this point.[9]

The power of the Cabinet or legislature to create a personal file outside the jurisdiction of the DIB is an example of several safety-valves in the legislation, which prevent the DIB from acting in a high-handed fashion on any specific measure.[10] Any decision of the DIB can also be appealed to the government (meaning in effect the Minister of Justice), but this happens infrequently (which is a tribute to the successful conduct of data protection by the DIB.)

The DIB enjoys and exercises a great deal of power. It has the authority to control the collection and dissemination of personal data, to regulate the usages of the resulting register, and to set up a system of responsible keepers for computerized data banks. It normally issues regulations concerning such matters as the "personal data which may be recorded in the file," and "the dissemination and other use of personal data."[11] The law itself establishes a detailed set of duties for responsible keepers of personal files.[12] There are also various types of civil and criminal penalties for breach of the Data Act.[13]

The DIB is an independent authority of the Swedish government with a Board of Directors, appointed for fixed terms, representing various political parties and interest groups. The Board was very involved in establishing basic policy for the direction of decisions in the early years, but most decisions are now made by the staff, which is headed by a Director General, who is also a member of the Board itself.

The Data Act has been amended in a minor way in 1979 and more substantially in 1982. In part, this illustrates the need to revise such a law on a periodic basis to reflect its experimental character and the fast pace of relevant developments in technology and society; the American Privacy Act of 1974, by way of contrast, has had only very minor revisions.

The revised law of 1982 has the goal of reducing the bureaucratic burden of data protection and of making the system of selective licensing of personal information systems self-supporting. These revisions occurred in response to the DIB's own internal assessment of what changes were necessary and the government's general desire to reduce the costs of government. It is noteworthy that the 1982 amendments passed by the margin of one vote, because of Opposition fears of appearing to weaken data protection. The revised statute instructs the DIB to exercise its supervision so "that it does not cause greater costs or inconvenience than is necessary."[14] Nevertheless, the small staff of the Data Inspection Board still finds itself swamped with work, because of the large number of automated registers in the public and private sectors that still require attention. The ambition of providing more time for staff to pursue the critical tasks of audits and inspections in order to ensure that the Data Act is in fact being observed in practice has not yet occurred. Moreover, charges for annual licenses have not generated enough income to make the DIB financially self-supporting. The staff resist becoming bill collectors as opposed to data protectors. Nonetheless, the Social Democratic government is committed to reducing expenditures on data protection.

The highly-politicized character of the continuing public debates over specific issues of data protection in Sweden indicate the sensitivity of the issues involved. Specific proposals to do new things with personal information regularly involve clashes between concern for efficiency and privacy. The debate that broke out in the summer and fall of 1983 over the the proposal for the 1985 census is simply a recent example; it led to national debates between the Director General of the DIB, Jan Freese, and the newly-appointed head of Statistics Sweden about the need for data protection in the field of statistics. Fortunately, the data protectors and statisticians are now discussing in private the many technical issues in data protection that arise in the field of statistics in Sweden.

The Social Democratic government has reduced sympathy for the goals of data protection, because of its (supposedly) conflicting goal of "catching economic criminals" involved in tax evasion and fraud. Jan Freese and his colleagues continue to defend the privacy interests of individuals in the face of various initiatives to (allegedly) save money or reduce fraud. Decisions of the Data Inspection Board are being challenged, with increasing frequency, by means of appeals to the Minister of Justice and the Cabinet, especially with respect to creating new record linkages. (In fact, the overall number of appeals remains very small.)

Jan Freese, who has been a senior staff member of the DIB since its inception and Director General since 1977, plays a crucial role as a publicist and activist for data protection. He appears regularly in the newspapers arguing for the right of privacy, warning about the consequences of record linkages, and so forth. If a high-quality, articulate, and activist Data Protection Commissioner is essential to the success of the enteprise, then Jan Freese (and Hans Peter Bull in West Germany) exemplifys the path to success.[15]

The state of data protection in Sweden after a decade of experience presents a series of problems. One starts with the fact that it has lost its novelty and some political support from the highest levels of the current government. Over time, this is a critical problem for data protection agencies in every country which has such an oversight mechanism. Fortunately, Opposition parties tend to be more supportive of data protection than incumbents. The national elections scheduled for September 19, 1985 may bring to power a coalition government with greater sympathy for data protection than the current generation of Social Democrats. A second issue is whether a staff of less than thirty persons at the DIB can really make data protection an effective force on an ongoing basis in both the public and private sectors. There is a risk in all countries of the general public receiving only the illusion of strong data protection. A third issue is whether data protection can be made financially self-supporting in both the UK and Sweden, as the respective governments intend. The bureaucratic burden of collecting annual license fees from users clearly detracts from data protection activities.

2.3 France:

The law of January 6, 1978 on Informatics, Data Banks, and Freedoms has an expansive and innovative character.[16] In particular, it illustrates the striking tendency for data protection to be defined in an all-inclusive fashion to cover a very broad range of societal issues that, from the perspective of English-speaking countries, go well beyond the protection of the privacy interests of individuals. In addition to the title of the statute, Article 1 best illustrates this point: "Informatics ought to be at the service of each citizen. Its development should occur in the context of international cooperation. It ought not to threaten human identity, the rights of man, private life, nor individual or public freedoms." Moreover, the National Commission on Informatics and Freedoms (CNIL), the agency set up to oversee the legislation, has set up four separate sub-commissions on such topics as freedom to work, research, local government, and freedom of expression. French data protectors believe that their mandate includes all of these concerns. One consequence is that their interests have wandered all over the map of contemporary French affairs and, at least to this point in time diluted the effectiveness of their achievements in data protection itself. One French response is the view that its expansive law is the wave of the future.

The 1978 law created an independent administrative agency with regulatory power, the National Commission on Informatics and Freedoms. It is a very novel institution under French law, being the first administrative agency with statutory independence from the government. The CNIL is obliged to ensure the observance of the 1978 law and to make decisions on the authorization of particular information systems in response to requests. The Commission has 17 members chosen for five-year terms by various official government bodies, including the Senate, the National Assembly, the Council of State, the Court of Cassation, and the Court of Financial Accounts. For the most part these bodies are truly independent of the government in the selection of their representatives. The speakers of the National Assembly and the Senate are empowered to select two persons qualified by their knowledge of informatics. Although the government itself has direct control of the selection of only three CNIL members, the two most recent presidents of the CNIL were drawn from among such appointees of President Mitterand.[17] France is a highly politicized society and the CNIL has taken on similar characteristics in selecting a President.

It is noteworthy that a member of the government or anyone engaged in the manufacture or provision of data processing or telecommunications services is disqualified from serving on the CNIL.[18] The government has direct input into CNIL decisions by the presence of its own representative who sits with the Commission and can, under the law, call for reconsideration of one of its decisions within a ten day period.[19] Such reconsideration never occurred until a few episodes in 1984, which may simply reflect another change in government commissioner. As part of a subsequent effort to make data protection more effective in the public sector, the government has created posts for data protection officials in each government agency. In so far as possible, the CNIL seeks to settle specific issues in data protection with these specialists.

The members of the CNIL elect their own president. Senator Jacques Thyraud was the president from 1979 to 1983; his successor was a newcomer appointed to the CNIL by President Mitterand, Monsieur Jean Rosenwald, a retired judge from the Cour des Comptes. (When the first five-year terms ended in the fall of 1983, seven new members joined the CNIL.) Rosenwald was elected president by a nine to eight vote in December 1983. After his untimely death in May 1984, he was succeeded by Mitterand's next choice, Monsieur Jacques Fauvet, the former director of Le Monde (1969-82). To an outsider, such results epitomize the politicization of the CNIL in line with the prevailing currents of political power in society. The usual explanation is that all of France is highly politicized and that, if the CNIL was to the right during the regime of Senator Thyraud and President Giscard d'Estaing, it is now to the left under the Socialists.

The experience of the CNIL to date suggests the problem of depending on part-time Commissioners for strong, affirmative implementation of data protection. The problem is whether such persons can devote the time necessary to develop appropriate expertise on pending issues. It is an issue that must be kept in mind in any proposal of a Data Protection Commission for the United States. Data protection has proved to be a difficult and complex task, requiring dedication and commitment, especially in the early years. If the DIB in Sweden illustrates the effective functioning of such a Commission system, led by a strong Director General, the reverse has been true in France. But there are indications that M. Fauvet intends to reverse this trend. He plans to appoint a Secretary General to coordinate staff activities; he also plans to study systematically whether recent decisions of the CNIL have been implemented in practice.

One of the surprising aspects of the CNIL is that it includes four elected politicians from the Senate and National Assembly, who can be expected to represent the majority in each body at the time of their election to the CNIL. Although this political element can be expected to sensitize the CNIL to political realities and even to strengthen the will of the body to take decisive actions when needed, such has not been the major result to date. In comparison to the Director General of the DIB or the Federal Data Protection Commissioner in West Germany, who are full-time persons, the CNIL was without a full-time President, or even a head of the professional staff, until January 1984. President Thyraud held several other positions which drew upon his time.

In France there have also been major problems of hiring, keeping and directing competent administrative staff who know how to administer and move mountains of paper in a system requiring the universal registration of personal information systems from both the public and private sectors. Because of the CNIL's independence, it was not obliged to recruit staff from the public service; thus patronage considerations played a not always positive role in the selection of staff. The two latest presidents are wisely committed to improving the quality and functioning of the staff of the CNIL, which totals about thirty-five to forty persons.

It is a problem for an agency such as the CNIL to find the will to resist the government on significant issues of information use by large public administrations. This issue raises the general question of the extent to which any data protection agency can resist any government's desire to use automated personal information for any purpose.

Critics argue that the CNIL has never taken a tough decision against the government with respect to a proposed new personal information system. Even though the 1978 law establishes that members of the CNIL "shall take no orders from any authority in the performance of their duties," their decisions have not been very adventurous.[20] The CNIL has rarely turned down a government proposal; perhaps wisely, it tends to negotiate changes during the process of application for approval. Moreover, because of the way it works in responding to specific requests for advice or declarations, the CNIL has not yet reviewed in detail all of the data banks that existed prior to the enactment of the 1978 law and has concentrated on proposals for new systems. This illustrates a basic flaw of the licensing approach: it prevents an appropriate focus on systematic and indeed systemic improvements in data collection activities, because those involved in the process are forever preoccupied with the specifics of any single application or modification thereof.

The risks exist in any country of providing only the illusion of data protection, with data protectors in fact serving as agents of legitimation for new forms and uses of information technology. Of the three countries discussed so far in this report, which have significant experience with implementation, this risk is greater in France than elsewhere.

Despite the several criticisms of the CNIL advanced here, its existence as an oversight and, in this case, regulatory institution has the very salutary effect of providing a forum before which issues of protecting personal privacy in an information society can be debated and resolved in incremental stages. Again the general point is reiterated here, because of the sharp contrast with the prevailing situation in data protection in the United States at the federal level.

A very recent event in France illustrates well how the CNIL serves a very useful function by the mere fact that it exists. On November 28, 1984 the satirical magazine Le Canard Enchaîné revealed that it had been able to penetrate the security net around the computers of the service bureau, the Compagnie Internationale de Services en Informatique (CISI), that has the French atomic energy agency as its major owner and client. Its agent used a mini-computer, a telephone, and a printer for this purpose and also obtained, in advance, the access code available to any of the thousands of clients of CISI; the purpose of the exercise was to test whether security was as impenetrable as the CISI had publicly claimed. The magazine claimed to have roamed at will among the data bases of the clients of CISI by usurping the identity of another user currently on the system; it published several columns of data which its agent obtained, taking certain precautions not to reveal the names of persons, which were blanked out. Le Canard claimed that the data bases of the clients of the CISI were as open to others as a public garden.

This news created a sensation in the French media, which are as interested in "hackers" and computer security as the press in other Western countries. In this case, the CISI complained to the CNIL against Le Canard, which presented the CNIL with the sensitive issue of how to handle an episode in which the press appears to be revealing personal data secured in an unauthorized fashion. Article 29 of the data protection law requires the maintenance of proper security in automated systems, a condition not apparently in place at the CISI. Article 43 of the same law forbids the publication of information that invades personal privacy. The data protection agency's first concern was to establish its legal jurisdiction in the matter, an approach typical of all of the continental European agencies in civil law systems. It then launched an investigation into the circumstances of the case, which could lead to criminal charges under the data protection law of January 6, 1978. If the facts seem to warrant criminal prosecutions, then the CNIL would simply refer the case to the appropriate prosecutors. The event at the

CISI also prompted the CNIL to acknowledge that it has not devoted enough efforts to computer security, especially at service bureaus, and to initiate various studies of its own in this area.

2.4 The United Kingdom:

In 1982 the government of Prime Minister Thatcher committed itself to go forward with data protection legislation along the broad lines of the European model in order to conform with the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[21] The motivation was economics and not human rights.

The Data Protection Act 1984 became law on July 12, 1984 and will gradually become fully operative over the next three years. It is a complex piece of legislation that establishes, among other things, an independent Data Protection Registrar with a staff of twenty to thirty non-civil servants, who shall maintain a register of personal data users and computer bureaux in the public and private sectors.[22] Although the Home Office emphasizes that the bill requires simple registration of automated systems rather than licensing, as in the Swedish and French models, it remains to be seen whether there are any practical differences in terms of large amounts of bureaucratic paperwork.

An entry in the Data Registry with respect to a data user has to include the following particulars: a) name and address of the data users; b) "a description of the personal data to be held by him and of the purpose or purposes for which the data are to be held or used;" c) "a description of the source or sources from which he intends or may wish to obtain the data or the information to be contained in the data;" d) "a description of any person or persons to whom he intends or may wish to disclose the data;" e) "the names or a description of any countries or territories outside the United Kingdom to which he intends or may wish directly or indirectly to transfer the data;" and

f) addresses for the receipt of requests from data subjects for access to the data.[3] Data users have to be registered and have to keep the particulars of their entries up-to-date. There will be a fee required for every application for registration and for each alteration of any particulars included in the entry.[24] It is the intention of the British government to make the system of data protection financially self-supporting. A government department which holds personal data will have to register with the Registrar as a data user.[5]

Schedule 1 of the Data Protection Act sets forth eight data protection principles; the duty of the Registrar shall be to perform his functions so as "to promote the observance of the data protection principles by data users and persons carrying on computer bureaux."[26] The principles resemble the fair information practices contained in all general data protection laws.

Part II of Schedule 1 provides guidance on the interpretation of the data protection principles, including guidance on whether information was obtained "fairly." In order for personal data to be treated as held for a specified purpose or as used or disclosed for a particular purpose, the particulars have to be included in the Registry. The information on interpretation of the principles also contains a useful exclusion for personal data "held for historical, statistical or research purposes and not used in such a way that damage or distress is, or is likely to be, caused to any data subject."[27] The latter provision changes the standard rules on informed consent to new data uses and on prolonged storage of data.

Section 5 of the Data Protection Act makes it a criminal offense to hold personal data without being entered in the register or knowingly or recklessly to hold, use, obtain, disclose or transfer such data otherwise than as specified in the registered entry.[28] The Registrar may refuse to register a data user, if he or she is satisfied "that the application is likely to contravene any of the data protection principles."[29] Alternatively, a user could be de-registered for non-compliance with the same principles.[30] Data subjects have the right to be informed that data about them have been collected, and the right to sue for damages if their data are disclosed by a data user or a computer bureau authority.[31] An appeal is possible from a decision of the Registrar to the Data Protection Tribunal and, ultimately, to the courts.

The British decision to move towards the model of a European-style data protection commissioner, even if done for purely economic reasons of permitting transborder data flows, has significant implications for the United States. To date, the American federal government and states have been able to argue that a Data Protection Commission or Commissioner was not in the English common law or legislative tradition, particularly in terms of giving such an official independence from the government (the Executive branch in U.S. language). It should now be more difficult to resist the creation of federal and state systems for data protection that include effective oversight mechanisms, along the lines of the 1983 New York Personal Privacy Protection Law, which came into effect on September 1, 1984. The existing state Committee on Open Government monitors the implementation of the provisions of the New York law.

Now it is also arguable that the U.S. federal government requires a Data Protection Commission to represent and protect the interests of American agencies, firms and individuals engaged in transborder flows of personal data. The U.K. Registrar is the designated authority under Article 13 of the Council of Europe Convention, which requires parties to have an authority to "furnish information on its law and administrative practice in the field of data protection."[32] A liaison function is obviously intended among data protection authorities in various countries. Since Europeans and Canadians already find it hard to comprehend the absence of such a credible authority in the U.S., the entry into force of the Convention, with its accompanying Consultative Committee of national representatives of each party to the Convention, will further increase the need for U.S. action. Whereas the OECD Guidelines recommend voluntary self-regulation, the Convention is a binding treaty among the parties, which already number fifteen signatories and five ratifiers. Non-European Nations may also be invited to accede to the Convention.[33]

The government appointed Eric J. Howe as the first Data Protection Registrar in September 1984. His main office will be located in Manchester, where he has worked since 1966 as a senior executive of the National Computing Centre. Howe expects the Data Protection Act to be proclaimed in force by September 1985. His current preoccupations are hiring staff, locating premises, designing registration forms, consulting with groups of users, and retaining a computer service bureaux to maintain the Data Protection Registry. About 200,000 registrations of users are anticipated. He expects to issue general guidelines on the implementation of the statute early in 1985. One of Howe's goals is to keep the process of registration relatively simple by designing forms with standard boxes to be checked off and with some room for narrative information to cover exceptional cases.

To this point in time, Howe has been receiving good notices from those previously involved in the development of British data protection legislation, but it is clearly too early to tell how his office and the law will work in practice.

2.5 Canada:

The relevant data protection legislation in Canada is the federal Privacy

Act of 1982, which supplanted and significantly strengthened the privacy provisions in Part IV of the Canadian Human Rights Act of 1977.[34] The latter introduced principles of fair information practice in the federal public sector (significantly influenced by the U.S. Privacy Act) and also created the post of Privacy Commissioner. Despite the title, the position is in effect that of a Data Protection Commissioner. The powers of the Commissioner consisted primarily in responding to complaints from individuals about denials of individual access to government personal data, until the 1982 law considerably strengthened the general powers of investigation and monitoring and set up a separate Office of the Privacy Commissioner. The 1977 law had the Privacy Commissioner as a member of the Canadian Human Rights Commission.

Sections 4 to 10 of the Canadian Privacy Act basically regulate the collection, retention, disposal, protection, and disclosure of personal information held by the federal government by means of a code of fair information practices. Its provisions are essentially similar to the American Privacy Act. The latter's concept of a "routine use" appears as a requirement that a government only use or disclose personal information "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose."[35] The Canadian law also specifies a list of thirteen purposes for which a government institution may disclose personal information.[36]

Although some of the disclosure provisions appear very broad, Treasury Board Canada, which has responsibilities comparable to the U. S. Bureau of the Budget, has produced an administrative policy guide to the entire Privacy Act, which gives the public service detailed interpretations of the intended meaning of each section in the statute.[37] The document runs to more than 100 pages and lends considerable support to a strict interpretation of the Privacy

Act in the direction of actually implementing appropriate measures for data protection.

The President of the Treasury Board is responsible for publishing an annual index of all the personal information banks maintained by the federal government in both manual and automated form, including the fewer than twenty-five banks that are exempt from access by individuals.[38] Each description is reasonably detailed and includes "a statement of the purposes for which personal information in the bank was obtained or compiled and a statement of the uses consistent with such purposes for which the information is used or disclosed."[39]

Aggrieved individuals can bring complaints about denials of requests for access to information to the Privacy Commissioner and ultimately to the Federal Court of Canada. But, more importantly, a person may complain to the Privacy Commissioner about any alleged form of personal information misuse by the federal government. Moreover, the Commissioner has the significant power and resources, including trained investigators, to initiate and investigate a complaint himself, where he "is satisfied that there are reasonable grounds" to do so.[40] In 1983 the Privacy Commissioner had to handle a highly-publicized complaint from a Member of Parliament that Revenue Canada Taxation was seeking broad access to all of the computerized records of the City of Kitchener, Ontario. Although he determined that the complaint was unfounded, it led him to warn against general "fishing expeditions" for records and uncontrolled computer matching.

Thus the Privacy Commissioner has an overall responsibility to monitor the implementation of the Privacy Act; in this important sense, he has no real counterpart under the comparable American statute. His recommendations to government departments are likely to carry a considerable amount of weight, although he does not have regulatory power, because he is an independent officer of Parliament. He can request a response from a department to one of his recommendations.[41] Even more importantly, he prepares an annual report to Parliament on the activities of his office and may also make special reports on "any matter within the scope of the powers, duties and functions of the Commissioner...."[42] The act directs that a permanent committee of Parliament should review the administration of the statute, which will provide the Commissioner with a specific sounding board for his views.[43]

Although the responsibility for implementing the Privacy Act is shared by the Treasury Board, the Department of Justice, and the heads of specific government departments, it falls to the Privacy Commissoner, Dr. John W. Grace, and his staff to make the law truly effective. In particular, this requires such positive initatives on the part of the Privacy Commissioner as carrying out supervision, audits, and inspections of federal personal information practices. After considerable delays in obtaining full-time permanent staff through Public Service competitions, this process of implementation is now beginning. The first audit of the personal information practices of a particular government department occurred in the fall of 1984. As in other countries, data protection requires action to be successfully implemented; waiting to help people who are having problems with requests for access to their own records is not a recipe for success; fortunately, Dr. Grace is well aware of this point.

The Privacy Commissioner holds office for a period of seven years and is eligible for re-appointment once. His independence is assured, at least in theory, by the fact that he is an officer of Parliament and is appointed by resolution of the Senate and House of Commons.[44] In practice, the initial selection is in the hands of the government of the day; thereafter, the

Privacy Commissioner has to retain the confidence of these two legislative bodies. Some problems could arise under the Canadian parliamentary system where the government controls the House of Commons. It is perhaps fortunate at present that the Progressive Conservatives dominate the Commons, while the Liberals prevail in the Senate. It would require an address (resolution) of the Senate and the House of Commons to remove the Commissioner from office.

At present, the Information Commissioner, who is responsible for the law on access to Government information (which is admirably integrated and coordinated with the Privacy Act), and the Privacy Commissioner share certain administrative staff in the same office. The Privacy Commissioner has a legal advisor, a director of complaints (plus five investigators), and a director of compliance (plus three investigators). The total is fifteen direct staff and a share of eighteen others.

Québec is the only province in Canada that has successfully introduced data protection legislation for the public sector, setting up an oversight and regulatory commission along the lines of existing European data protection models. Quebec passed Law 65 in June 1982 on the basis of the recommendations of the Paré Commission Report of 1981.[45] The three members of the independent supervisory Commission d'accès à l'information, whose responsibilities include overseeing the protection of privacy in the public sector, were appointed by the National Assembly in December 1982. The first eight of the 180 articles in the Quebec law took effect on October 1, 1982; the privacy provisions became effective (with one exception) on July 1, 1984. The Quebec law incorporates the standard provisions for fair information practices usually found in data protection laws. Thus personal data collected by a public body have to be necessary, accurate, timely, and complete.[46]

Québec's Law 65 has a very broad scope. It applies to the personal-information handling activities of all public bodies, including municipalities, schools, universities, and health and social services, a total of more than 3,500 public bodies.[47] Each has to submit a declaration to the Commission concerning the establishment of all personal information files. Based on the experiences of France and Norway in particular, there is a significant risk that this requirement will overwhelm the Commission with routine paperwork and perhaps make active supervision and inspections impossible. The Commission does have significant powers to supervise all aspects of the law, to prescribe conditions for a personal file, to advise on proposed agreements covering the transfer of information, to respond to complaints or conduct its own investigations, and to issue binding orders to a public body to "correct, complete, clarify, update or delete any nominative information, or discontinue the use or release of nominative information."[48] There are various criminal sanctions for breach of Law 65.[49]

2.6 Australia:

The Australian Law Reform Commission was given a broad mandate to consider a wide variety of privacy issues, including data protection, in April 1976. The Commission was asked to "inquire into and report upon: the extent to which undue intrusions or interferences with privacy arise or are capable of arising under the laws of the Commonwealth Parliament or of the Territories, and the extent to which procedures adopted to give effect to those laws give rise to or permit such intrusions or interferences..."[50] The Commission's inquiry covered privacy issues associated with "the collection, recording or storage of information by Commonwealth or Territory Departments, authorities or corporations, or by persons or corporations...," in addition to privacy aspects of powers of entry and search and seizure. The Commission was asked to make recommendations on legislative measures to fill any lacunae identified by its study. After an exhaustive inquiry and the publication of a number of specialized reports on specific isuues, a comprehensive three volume report was delivered at the end of of 1983. The Law Reform Commission concluded that "privacy is in danger, both in actuality and, even more so, in prospect."[51] At present, the newly-reelected Australian government is said to be preparing draft national legislation on data protection.

The conclusions and recommendations of the Australian Commission with respect to both privacy and data protection issues are reasonable, up-to-date, and compelling. Its balanced point of view vis-à-vis privacy is neatly summarized by the statement: "A scheme for its better protection, in order not to detrimentally upset the balance of competing claims achieved in various areas of legal and government administration where privacy interests have surfaced and been identified, must build upon the rules developed in those areas, and the experience of those who administer them."[52]

With respect to its recommendations for data protection legislation, the report acknowledges that the OECD Guidelines "have helped shape the Commission's recommended principles for data protection."[53] The Commission formulated ten general principles for privacy protection that correspond to the Guidelines, but also spell out the rights of data subjects in slightly more detail.[54]

The Commission expressed the view that personal information should be broadly defined as "information about a natural person from which, or by use of which, the person can be identified."[55] It rejected the licensing model for data protection but recommended the creation of a "statutory guardian" as is discussed below. In its view the private sector should come within the ambit of legislation.[56] It is not clear, however, what form the legislation will ultimately take; the Commission suggests simply that "a legislative statement of principles for privacy is clearly desirable. Wherever practicable, mechanisms to give legal force to the principles should be provided."[57]

Most significant for the purposes of this current report is the Commission's recommendation that a "statutory guardian, in the form of an administrative body with the specific function of advocating privacy interests" should be created under the auspices of the Human Rights Commission (HRC).[58] Thus the Australian Law Reform Commission has effectively endorsed the Canadian and European models of data protection. The Commission believes that a single individual, a "Privacy Commissioner," should be designated as a "specific, publicly identifiable person who has the primary responsibility for dealing with privacy complaints."[59] The report argues that, in addition to this ombudsman-like function, it is essential that "he be involved in the continuing task of formulating the standards and guidelines the HRC will issue. It will be necessary, too, for the HRC to use his experience while advising government."[60] Finally, the Commission notes that in its model the "Privacy Commissioner will play a significant part in monitoring and regulating the exercise of intrusive powers by Commonwealth officials."[61]

In a departure from data protection practices in most English-speaking countries, the Report suggests that the Commissioner should have regulatory power in one specific area, the handling of individual requests to obtain access to their own data and to amend incorrect records: "The Privacy Commissioner...will have the power to issue binding and enforceable orders. These orders will be appellable to the Administrative Appeals Tribunal.... He should be able, where appropriate resolution of any aspect of a dispute in relation to access or amendment of a personal record is not otherwise possible, to direct the record keeper to give access to, or to amend, the record concerned"[62]

In general, the basic functions of the Australian Privacy Commissioner will be similar to that of his or her counterpart in Canada and data protection officials in Western Europe. They are listed below in summary form as a guide to what is needed in the United States:

1. Inquiry into, and conciliation and resolution of, disputes;
2. Monitoring activity and technological advances that might interfere with privacy;
3. Fixing standards and publishing guidelines;
4. Providing community education about privacy; and
5. Advising government, industry and the processions.[63]

2.7 Japan:

In 1974 the Administrative Management Agency (AMA), a part of the Prime Minister's Office, began to consider the issue of data protection. In January 1981, the AMA established the Committee on the Protection of Privacy. It studied the present state of personal data handling and data protection in the public and private sectors, including the fields of medical care, banking and credit, insurance, and the information processing industries. The Committee focused on the OECD Guidelines, main privacy developments in OECD countries, and assessed privacy concepts and the interests they protect.[64]

The Privacy Committee's final report of July 1982 reflects the influence of the OECD. The report concluded that legislation to protect privacy was required and that it should ensure observance of the OECD principles of collection-limitation, use-limitation, individual- participation, proper-management, and accountability.[65] The Committee recommended that legislation should be enacted to deal with the public and private sectors and that manual records should come within its purview. More than anything else, the legislation recommended by the Committee's report appears to suggest primarily measures to implement the OECD Guidelines, which Japan has signed.

Notwithstanding the relatively uncontroversial nature of the Privacy Committee's recommendations, the AMA has yet to respond to the argument that legislation is required. It has been suggested that the action of the AMA on this issue reflects a desire to lay claim to the area in the event that it becomes important rather than a strong commitment to data protection.[66]

The AMA released a national opinion poll in September 1981 indicating that the Japanese are generally aware of issue of privacy and concerned about the impact of computers on privacy. However, it is felt that the issue has yet to take on substantial political ramifications; there have been no colourful invasion of privacy stories, and public opinion and industrial groups do not appear to be actively concerned about privacy.[67]

Therefore, it is not clear when, or if, Japan will enact data protection legislation. It is evident that, to the extent that the AMA reflects government policy, the orientation towards data protection will be primarily towards promoting the "free-flow of information."

Notes

1. The English text of the 1977 law can be found in the appendix. It is also printed in Ulrich Dammann, Otto Mallmann, and Spiros Simitis, eds., Data Protection Legislation: An International Documentation (Frankfurt am Main, West Germany, 1977), pp. 70-107; and in Rein Turn, ed., Transborder Data Flows (2 vols., Arlington, Va., 1979), II.

2. Ibid., s. 17(3) and s. 17(5).

3. Ibid., s. 19(1).

4. Ibid., 2. 19(2).

5. Ibid., 2. 20.

6. Ibid., s. 21.

7. Data Act, section 3. Unless otherwise noted, this discussion is based on the Data Act as amended with effect from July 1, 1982. See appendix 2 for the full text. Note that "a registered person" is an individual about whom data are stored in a data bank or register.

8. Ibid., s. 2. Like every other data protection law, the Data act is a complex document and relatively incomprehensible to the general public. An example is the list of criteria in section 2 for situations in which the actual permission of the DIB is needed to set up and keep a personal file.

9. Ibid., s. 4.

10. Ibid., s. 2a.

11. Ibid., s. 6.

12. Ibid., ss. 7-14.

13. Ibid., ss. 20-25.

14. Ibid., s. 15.

15. Recent examples of Freese's writing in English include: "The Right to be Alone in Sweden," Transnational Data Report, VI, No. 8 (December, 1983), 447-49; and "Freedom of Information and Privacy Protection in Sweden," in Pierre Trudel, ed., Accès à L'Information et Protection des Renseignements Personnels. Expérience Occidentale et Perspective Québeçoise (Montreal: Les Presses de l'Université de Montréal, 1984), pp. 13-26.

16. The English text of the law can be found in appendix 3. I have used my own translation of certain terms and phrases in various parts of this report.

17. Ibid., Article 8.

18. Ibid., Article 8.

19. Ibid., Article 9.

20. Ibid., Article 13.

21. Background information for the U.K. can be found in the slender White Paper: Data Protection: The Government Proposals for Legislation, Cmnd. 8539, London, UK, April 7, 1982. The Convention opened for signatures on January 28, 1981; it is expected to enter into force shortly, now that it has been ratified by the necessary number of nations, which is fixed at five.

22. Data Protection Act, sections 3-4. The statute may be found below in appendix 4. A valuable annotated edition has just been published by Bryan Niblett, Data Protection Act 1984 (London: Oyez Longman,1984). "Computer bureaux" are data processing services (section 1[6]). See also a speech by the Minister at the Home Office responsible for shepherding the Data Protection Bill through the House of Commons: David Waddington, "Protection of Personal Information in the U.K.: The Data Protectin Bill," in Rudy Wall, ed., Conference on Privacy: Initiatives for 1984. Toronto, Ontario, Canada. May

22-25, 1984 (Toronto: Ontario Provincial Secretariat for Resources Development, 1984), pp. 24-29.

23. Data Protection Act, s. 4(3). Niblett suggests that only a description or general indication of the particulars is required under subsection 3(b) to 3(e) rather than "the precise details." (Data Protection Act 1984, p. 28.) However, he subsequently recommends that the description in the register of the purposes for which data are to be held or to be used and the persons to whom they are to be disclosed should be "comprehensive" in order to comply with the interpretation of certain of the data protection principles in Schedule 1 of the Act. (Ibid., p. 99.)

24. Data Protection Act, ss. 6(3) and 6(7).

25. Ibid., s. 38(1).

26. Ibid., s. 36(1).

27. Ibid., Schedule 1, Part II, paragraphs 1, 2, 3, and 7.

28. Ibid., ss. 5(1) and 5(2). The act introduces fifteen new criminal offenses, which Niblett conveniently lists. (Data Protection Act, pp. 114-16).

29. Data Protection Act, s. 7(2)(b).

30. Ibid., s. 11(1).

31. Ibid., ss. 21(1)(a) and 23(1)(c). Niblett points out the Act provides five new civil remedies to the data subject and that these "are by no means negligible provisions." (Data Protection Act, p. 12 and the listing at pp. 117-18.)

32. Data Protection Act, s. 37. The text of the Convention may be conveniently consulted in Niblett, Data Protection Act, pp. 119-27.

33. See Niblett, Data Protection Act, pp. 5-7, 126.

34. An Act to enact the Access to Information Act and the Privacy Act, S.C. 1980-81-82-83, c. 111, schedule II. (Hereafter cited as the Privacy Act.) A copy of this legislation can be found in Appendix 5 of this report.

35. Privacy Act, ss. 7(a), 8(2)(a).

36. *Ibid*., S. 8(2).

37. Treasury Board Canada, *Interim Policy Guide: Access to Information Act and the Privacy Act* (Ottawa: Treasury Board Canada, June 1, 1983.) Public servants also receive continuing direction in the application of the statute from the Information Law and Privacy Unit of the Department of Justice and from the Information Policy unit, Administrative Policy Branch, Treasury Board Canada.

38. The most recent edition is Government of Canada, *Personal Information Index 1984* (Ottawa: Minister of Supply and Services Canada, 1984). These listings have been published since 1978, and their detailed coverage has improved over time. The current edition runs to about three hundred pages. Copies are available in post offices and libraries across Canada, but it is unusual to find persons who have consulted them.

39. Privacy Act, s. 11(1)(a)(iv).

40. *Ibid*., ss. 29-30; see also s. 37(1) concerning the Commissioner's power to carry out investigations to "ensure compliance with sections 4 to 8" of the Privacy Act. Some valuable insights into the perceptions held by Dr. John W. Grave, the incumbent, can be found in his first annual report: Privacy Commissioner of Canada, *Annual Report, 1983-84* (Ottawa: Minister of Supply and Services Canada, 1984), passim.

41. *Ibid*., s. 35(1)(b).

42. *Ibid*., ss. 38-39.

43. *Ibid*., s. 75(1). This activity will be carried out by a subcommittee of the House of Commons' Standing Committee on Justice and Legal Affairs.

44. Ibid., ss. 53(1)(2)(3).

45. Québec, Information et Liberté. Rapport de la Commission d'étude sur l'access du citoyen à l'information gouvernementale et sur la protection des renseignements personnels; An Act respecting access to documents held by public bodies and the protection of personal information, R.S.Q. chap A-21.The new Québec law is discussed in detail in Pierre Trudel, ed., Accès à L'information et Protection des Renseignnements Personnels. Expérience Occidentale et Perspective Québéçoise (Les Presses de L'Université de Montréal, Montréal, 1984), especially chapter 6.

Bill 80, An Act to provide for a Right of Access to Government Information in Ontario and to provide Protections respecting the Collection and use of Personal Information, received first reading in the Ontario legislature on May 24, 1984, but speedy passage is not expected. See Rudy Wall, ed., Conference on Privacy: Initiatives for 1984, Toronto, Ontario, Canada. May 22-25, 1984 (Ontario Provincial Secretariat for Resources Development, 1984).

46. R.S.Q., c. A-21, ss. 64, 72.

47. Ibid., ss. 3, 5-7.

48. Ibid., ss. 76, 123(1), 123(3), 124, 128 and 141.

49. Ibid., ss. 158-65.

50. Australia, The Law Reform Commission, Privacy. Vol I: Background. Report No. 22. 3 vols. (Canberra: Australian Government Publishing Service, 1983), p. xxxvi.

51. Ibid., p. xli. The Australian study of privacy is the most comprehensive and exhaustive evaluation currently available on all aspects of the subject.

52. Australia, The Law Reform Commission, Privacy. Summary of Report.

(Canberra: Australian Government Publishing Service, 1983), p. 3.

53. Ibid., p. 8. Mr. Justice Michael Kirby chaired the Committee of Experts that drew up the OECD Guidelines; he also chairs the Australian Law Reform Commission.

54. Australia, The Law Reform Commission, Privacy. Vol. 2: Proposals. Report No. 22. 3 vols. (Canberra: Australian Government Publishing Service, 3 vols., 1983), paras. 1193-1385. The Report's discussion of issues associated with its data protection proposals is very comprehensive.

55. Ibid., para. 1198.

56. Ibid., para. 1202-1206.

57. Ibid., para. 1201. This volume includes, as Appendix A, a Draft Privacy Bill, which treats all aspects of the subject, including data protection. The Draft Bill runs to fifty pages; there are another eighty pages of notes to the Bill and proposed draft amendments to other relevant legislation.

58. Privacy. Summary of Report, p. 22.

59. Privacy, Vol. 2: Proposals, para. 1059.

60. Ibid., para. 1062.

61. Ibid., para. 1106.

62. Ibid., para. 1065.

63. Ibid., para. 1040.

Japan

64. "Japan Readies Privacy Protection Policy," Transnational Data Report IV(No. 8, 1981); p. 1.

65. "Japan Prepares National, Local Privacy Measures." Transnational Data Report VI(No. 3, 1983); p. 125. See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1981.)

66. T. Hiramatsu, "Japan's Privacy Protection Measures," Transnational Data

Report VII(No. 2, 1984); p. 109.

67. Ibid.

3. Record Linkages: Computer Matching and Computer Profiling

In this chapter, and the next ones, certain specific problems of data protection will be discussed, because they are of particular interest to the Office of Technology Assessment's study of federal information technology and because they are issues that concern data protectors in all of the countries that have data protection laws. This particular chapter looks at a group of associated issues that can be roughly described as record linkages, computer matching, and computer profiling. The critical term is in fact record linkages, because one is in fact focusing on the use of computers to integrate discrete items of personal information from separate personal data systems. The term "computer matching" is in fact the descriptive phrase used in the United States to describe a particular problem, which in certain ways is more advanced (or at least less controlled) in the United States than in other countries for both political and technological reasons, including the will to catch "welfare cheats," the lack of an adequate oversight mechanism to regulate such practices, and the ready availability of automated data bases for linkage purposes. As noted elsewhere in this report, such pressures and conditions also exist in other countries. The United States has paid significant attention to date to the computer matching as a problem at both the federal and state levels.[1] Because of American influence, the Canadian Privacy Commissioner has also described computer matching as a potential problem.[2]

What Americans must keep in mind, however, is that such issues as computer matching and record linkages are automatically caught up in the normal net of data protection activities in European countries and in Canada. Jan Freese, the Director General of the Swedish Data Inspection Board, has long been concerned about record linkages; in fact, he is among the few who have made the critical point that poor data quality is a basic argument against permitting record linkages for administrative purposes.[3] In general terms, the European data protection laws require advice or consent for government record linkages.

At the opening of his hearing in December 1982, Senator William Cohen defined computer matching as "the comparison of different lists or files to determine whether identical, similar, or conflicting information appear in them. Comparisons can be made by matching names, social security numbers, addresses, or other personal identifiers." He noted that technology was facilitating and speeding a process that was previously possible by manual means, and that computer matching brought into conflict such values as the protection of privacy and the detection of fraud and mismanagement in government programs.[4]

It is essential to note at the outset of this discussion that computer matching or record linkages for administrative purposes are in no way inherently a bad idea. In fact, as I have noted elsewhere, there is a congruence between the goals of computer matching and data protection at the level of the use of matching as an editing function to reduce data collection and to remove "pollution" in the form of inaccurate data from government personal information systems.[5] Moreover, privacy advocates normally do not resist "up-front" matching, which occurs at a point where a person applies for a particular government benefit or program, for which he or she claims to be qualified. It is appropriate to determine whether an individual is in fact unemployed, has in fact undergone a medical procedure, or has a certain level of educational attainments. Matching may also make an essential contribution to the auditing function.

The serious problems in record matching begin in situations where automated data collected for a specific purpose by one arm of a government are used for a new administrative purpose, often by another arm of a government, without the informed consent of the person concerned.[6] The special need in controlling computer matching is to create an oversight mechanism, such as a Data Protection Commission, which can help to establish an acceptable balancing of competing societal interests by articulating privacy values in a coherent fashion. There is a need, in the United States in particular, to establish standards and limits for computer matching and, then, to enforce them. The experience of the United States and of other western countries suggests that it is ill-advised to rely on courts to monitor and control such a complicated and specialized activity. The remainder of this chapter will discuss progress to date in other countries in achieving the necessary controls and standards for record linkages. Dr. John W. Grace, the federal Privacy Commissioner, chose to discuss the threat to a citizen's privacy rights posed by the technique of linking computer files in his first annual report, which was released in early July 1984: "The surreptitious matching of personal information collected for different purposes and contained on different computers could be as destructive of privacy as wiretapping telephone conversations."[7] Although no evidence of improper computer matching has come to his attention, Grace noted that the Privacy Act of 1982, which is otherwise silent on the specific topic of computer matching, contains the basic principle that information should only be used for the purpose for which it was collected.

3.1 Canada

The Canadian Privacy Commissioner recognizes the mounting pressures to use computer matching as a standard investigatory technique to catch tax evaders or welfare cheats: "That computer-matching is carried on in the name of efficiency, good government and law enforcement makes it potentially a more, not less, dangerous instrument in the state's hands."[8] It is particularly instructive that Grace chose to use his first annual report to make a strong statement about this particular problem of computer matching. He described "covert computer linkage with unauthorized data matching" as a form of search and seizure worthy of alarm and requiring procedural safeguards; otherwise, "there is the danger that these computers will, of course, function mindlessly and without discrimination, as mere machines must do."[9]

Thus both the Privacy Commissioner and other information policy specialists in the Canadian federal government regard computer matching as an emerging issue worthy of serious attention. Some public servants believe that there is considerable movement at present towards the increased use of matching, especially using federal government employee records. Some supervisors want to use records of drinking episodes in grievance procedures. There are pressures from management to use matching for improved selection of personnel for positions.

Proposals to open federal data banks to obtain information for collecting alimony and child support payments from recalcitrant fathers are also going forward, including plans for access to some government personal information systems for tracking purposes. The main need is to obtain current addresses for the persons in question, and the government proposals expected early in 1985 will be limited to granting acess to this item of data. Federal Justice Minister John Crosbie explained on November 23, 1984 that "there is no sinister Big Brother connotation of electronic and mysterious means of ferreting out intimate details of anyone's life.[10]

It was recently revealed that in 1979 Revenue Canada officials used a provincial voters' list from the province of Prince Edward Island to match with their own tax records in order to identify individuals who had not filed income tax returns.[11] In this case Revenue Canada officials, who could not explain how the typewritten voters' list was obtained, had to keypunch the new data rather than using an existing magnetic tape. The newly-appointed Minister of Revenue for the Progressive Conservative government, Perrin Beatty, has asked his officials to report to him on all prior episodes of matching with personal data obtained from outside his agency. Because of Beatty's record of concern on issues of privacy protection, his stewardship of Revenue Canada will make public servants very wary of engaging in any kind of computer matching without ministerial clearance.

The most recent revelations about computer matching concerned the activities of the Canada Employment and Immigration Commission (CEIC). At a Science Council of Canada conference in Ottawa on October 2, 1984, B. K. Dertinger, the executive director of systems and procedures at CEIC, described the matches that they routinely carry out. In general, they fall into the category of up-front matches that privacy advocates can hardly complain about. (Nor, to this point in time have they even known about them.) CEIC is especially concerned to discover overpayments of unemployment insurance benefits and uses only employment-related data to do the matching. CEIC uses its Social Insurance Number Index (the SIN number is equivalent to the Social Security Number in the U.S.), covering 25 million persons, as the unique personal identifier for all claimants for unemployment insurance. The records of employment for each worker are maintained by SIN and furnished to CEIC by employers. Payments for unemployment insurance are matched against records of employment.[12]

According to CEIC, its internal matches of data are authorized by various statutes and section 8(2)(a) ["consistent use"] of the Privacy Act. It makes the usual claims of a large number of "hits" and of substantial savings to taxpayers. In addition, as described in the relevant Personal Information Index, CEIC exchanges welfare data with the provinces "to allow various social agencies under their control to verify the entitlements of their clients with the Commission."[13]

One conclusion that can be ventured for this Canadian discussion is that the entire process of matching by federal agencies can and, indeed, should be monitored by the Privacy Commissioner. As noted earlier, he has only recently acquired full-time staff on a permanent basis and begun the process of systematic checking on the extent of compliance with the Privacy Act within individual departments. As the London Free Press argued in a recent editorial, "before the practice of computerized matching of data banks becomes a full-blown industry, a great deal of thought should go into the propriety of such techniques," including the formulation of a code of ethical practices and a detailed protocol on computer investigations.[14]

3.2 Sweden

Because Sweden has so many automated personal registers in both the public and private sectors, and because each citizen is uniquely identified by a Personal Identification Number (PIN), there are constant proposals to create record linkages for large and small purposes. There have even been plans to link all important computer files of personal data in Sweden. Fortunately, the Data Act generally requires that all such plans be licensed through the Data Inspection Board (DIB). In fact, according to section 2 of the Data Act, specific permission is required from the DIB for the linkage of files which are to contain "personal data procured from any other person file, unless the data are recorded or disseminated by virtue of a statute, a decision of the Data Inspection Board, or by permission of the person registered."

Jan Freese, as noted earlier, is the most ardent foe among data protectors and privacy advocates of record linkages. Perhaps because Sweden is in fact a paradise for automated data banks, he has strongly resisted various linkages proposed by government agencies in particular.[16] Freese, and at least certain members of his Board, are concerned about the real prospects of creating a society in which computers keep everyone under complete surveillance. He argues that a society which developed a workable scheme to end all tax frauds would be an impossible place for persons to live in. He is also very emphatic about the risks of linking together records for decision-making purposes which are in fact of inadequate quality to protect against mistakes and errors.

There appear to be much more substantial flows of personal data among the state, municipal governments, and the private sector in Sweden than in other countries. Freese describes it as "no longer a case of two-way communication but of multi-way communication. In few other countries, if any, can, for example, the insurance companies be linked computer-to-computer with the Motor-Car Registry, or even with a centrally run population file. In Sweden it is even possible for a private car dealer to link up via a terminal with the Motor-Car Registry, or for a state authority to 'plug in' in the same way to the files of a private credit information company."[15]

At the same time, Freese and his colleagues at the DIB emphasize that they are not hostile to all forms of record linkages or computer matches. One estimate is that eighty to ninety percent of the record linkages that are proposed to the DIB are approved as satisfactory and acceptable. The DIB is resistant to linkages in which the users do not know why the personal information was collected in the first place or are seeking to link very sensitive personal information, such as linked data on alcoholics and drug addicts. The risky linkages are those that are carried out to exercise control (surveillance) over the population or in order to avoid direct collection of information from individuals. (It is not clear from the Swedish use of the word "control" in English, whether the DIB is referring to up-front matching or matching at a period of time substantially later than the time of a particular transaction.) Freese notes that he has no problems with conducting linkages for purposes of updating a file, such as changing the address of an individual. His main concern, and it seems a most sensible one, is with the quality of the data used in record linkages. One has to know when, why, and how the data were collected before any linkages can be attempted. Freese points out that one can hardly do successful record linkages on the basis of poor medical diagnoses, for example: "Unless one knows from whom, when, how and why the data were compiled, the linked processing will be misleading. Unfortunately, the DIB has only too often come across instances where linking of various data submitted at various times for various purposes has made the most honest of persons look like a crook."[16]

Freese has particularly aroused the ire of the Social Democratic government by opposing many of their proposals to use record linkages to exercise "controls" over the population, especially for apprehension of what are called "economic criminals;" the latter category includes tax evaders and other white-collar criminals.

The DIB points out that the pressure for more record linkages in Sweden comes from administrators and not data processing specialists, who tend to be more aware of the problems of data quality. One example used is that persons planning linkages need to be aware of the actual meaning of a net income figure for a particular person before using the data elsewhere. The net income figures for tax purposes may not be relevant or have a suitable meaning for a third use. There seem to be no problems in linking hard facts about an individual, such as a birthdate, but it should be impossible to link soft information, which has to be turned into hard "facts" for purposes of linkage. It is a hard fact that a person drinks a quart of alcohol a day, but it is a soft fact to classify someone as an alcoholic. This illustration is useful in explaining the resistance of the DIB to record linkages.

The important point for present purposes is that almost all record linkages in Sweden are subject to regulation by the DIB. This is not to suggest the DIB is always successful. For example, the taxation authorities are seeking all available automated data held by Swedish banks on income from interest and dividends received by individuals. When the banks ask the DIB if this was possible under their license from the DIB, the latter said no, but the banks gave the personal information to the tax authorities anyway. The DIB sought to prosecute the banks under the Data Act, but the case was dropped by the prosecutor assigned to the case. The highest level of state prosecutor is now deciding whether this was a legitimate decision. The tax authorities would like to create a taxation system based on automated access to existing administrative data bases in the private sector. They want to avoid licensing by the DIB, which is itself resistant to the creation of a society in which individuals are even more controlled and regimented. In the Swedish system of data protection, the ultimate resolution of such a clash of values has to be made by the government; but, like all of the other countries treated in this report, Sweden has a system in which the privacy interests of individuals are well articulated by the Data Inspection Board during such a process.

3.3 France

The French CNIL functions in a manner similar to the Swedish DIB in terms of having to authorize record linkages in specific cases that are brought before it by applications. Because of its preoccupation with the principle of finality (personal data should only be used for the purposes for which they were collected), the CNIL is generally hostile to secondary or unintended connections of information. But, generally, plans for record linkages between government departments, information systems within one agency, appear to be relatively underdeveloped in comparison to other countries.

Moreover, because of the strong terms of the law of January 6, 1978, the CNIL has even more reason to be sensitive to certain types of linkages. Article 2 of the law specifically seeks to control computer profiling: "No judicial decision involving an appraisal of human conduct may be based on any automatic processing of data which describes the profile or personality of the person concerned. No governmental or private decision involving an appraisal of human conduct may be based solely on any automatic processing of data which describes the profile or the personality of the person concerned." This is the strongest measure of its type in any national data protection law. It is further strengthened by Article 3: "Any person shall be entitled to know and to dispute the data and logic used in automatic processing, the results of which are asserted against him." Such measures are designed to promote what Europeans term the transparency or openness of society. Article 26 adds that, in most cases, "any natural person is entitled to object, for due cause, to the processing of personal data concerning him." The CNIL thinks that credit companies are ignoring these measures concerning computer profiling in their preparation of credit scores. When one company refused to divulge its plans and computer programs to the CNIL in 1984, it held a hearing and launched an investigation, which may lead to new general rules for the credit industry under the data protection law of January 6, 1978.

3.4 United Kingdom

Although there is no experience to date with the problem in the U. K., it is useful to examine how the Data Protection Act of 1984 is designed to cope with computer matching and record linkages. In the first place, a government department holding personal data, or offering data processing services as a computer bureau, will have to register with the Registrar. Thus, as Bryan Niblett points qut, "an intention by one department to disclose personal data to another will have to be included in the register under s 4(3)(d)."[17] Thus the Registrar will know about transfers and proposed or existing linkages and may evaluate their validity in the light of data protection principle three: "Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."[18]

Niblett, who is both a barrister and a computer scientist, has drawn attention to the risks of what he calls an "inverted file, that notorious source of many of the fears for personal privacy that data processing engenders."[19] He is referring to "combinations and associations of data elements" in a file of data inverted to bring together "the addresses of all occurrence of the same data element." He uses the benign example of a concordance to every use of a word in the Data Protection Act, which actually appears in his edition of the statute: "This technique of file inversion...is clearly of remarkable power, and not always harmless, when applied to personal data files used for such matters as hotel registration, vehicle licensing and criminal intelligence."[19] Niblett's concerns are particularly noteworthy, because he is definitely not a member of the "alarmist" school of data protectors.

3.5 Federal Republic of Germany

As in the other countries covered by this study, pressures are growing in West Germany to use computer-matching techniques and the linkage of records in the interests of efficient use of time and resources. The West Germans have used computer matching to respond to the wave of German terrorist activities in the late seventies. But they have also subjected the process of matching to principles of data protection.

The Republic's Federal Data Protection Act contains in subsection 10(1) a general prohibition against the dissemination of personal data from one public body to another, unless the release of the information "is necessary for the legitimate accomplishment of the tasks for which the dissemination unit or the recipient is competent." Because the Act contains no provisions dealing expressly with computer matching, record linkages or personality profiles, the above principle has to take its concrete form in specific sections of statutes for specialized forms of information handling and in regulations passed thereunder.

Government information in the field of social services is within the statutory purview of the Social Code. The Code contains in subsection 35(1) of Book One a broad right of an individual to have personal and business information on him held by social benefits agencies protected under what is known as 'social secrecy.' Exceptions are provided in sections 66 to 77 of Book Ten, which essentially permit the internal use of data for purposes of social administration, other than any data collected by a doctor, which information is given very strict protection under section 76 of Book Ten.

Essentially, if a social agency seeking non-medical information is fulfilling legal tasks and the information is essential to those tasks, as specified by statutes or regulations, then the social agency from whom the information is requested may transmit its information to the requesting agency, and the latter "may even pose questions to determine whether an individual has received or applied for social benefits."[20] Within the above limitations, computer matches and record linkages among social service agencies appear unrestricted. They do not even have to be reported to the

Data Protection Commissioners.

Although the Social Code prevents most information transfers to parties outside of the social administration, the data banks of the social services can be linked to those of other government agencies under section 71 of the Social Code, Book Ten, in one or more of three situations; first, to prevent premeditated crimes - and there is a corresponding duty to provide this information under section 138 of the Criminal Code (Strafgesetzbuch); secondly, to protect public health under the Federal Epidemics Act (Bundesseuchengesetz) or under the Act to Combat Venereal Diseases (Gesetz zur Bekämpfung von Geschlechtskrankheiten); and, thirdly, to implement the taxation process pursuant to sections 93, 97 and 116 of the Tax Ordinance (Abgabenordnung). In effect, this third situation places the social administration under a duty to provide records to the finance administration on social welfare benefits in order to match them with tax records.

In the spring of 1982 the Bundestag passed another exception to the rules preventing the matching or linking of social data bases with the data bases of government agencies outside of the social administration. The target was aliens living in the Federal Republic. Information on the receipt of social assistance can now be transmitted to the registered alien authorities to determine whether certain activities of these persons are within the law. Each social benefits agency first determines "whether and to what degree the data are essential to determine that the alien has deceived the administration, that he 'endangered public health or morality' or that 'he cannot pay or is not paying for the maintenance of himself and his dependents whom he is obligated to support without resort to social assistance," and then transmits such information to the registered alien authorities. Each of the above grounds is sufficient to warrant deportation.[22]

The Social Code makes specific provision for transmitting information from social benefits agencies to the security authorities. Social data can be released, under section 72, paragraph 1, sentence 1 of the Social Code, Book Ten, in connection with investigating serious premeditated crimes "as far as [the release of information] is essential in the individual case for completing duties, pursuant to law, within the jurisdiction of the Agencies for Protection of the Constitution, the Federal Intelligence Service, the Military Counter-Intelligence Service and the Federal Office of Criminal Prosecution." The same section also restricts the information to "details of given name and surname, date of birth, current and previous addresses of the person concerned as well as names and addresses of current and previous employers." Professor Hans Peter Bull, the former Federal Data Protection Commissioner, explains that this section prevents the release to the security authorities of information on what social benefits someone is receiving or the state of a person's health, and, furthermore, argues that if this section is correctly interpreted, it prohibits the pattern-search technique discussed below, from being applied to data bases of the social benefits agencies.[23]

The Federal Office of Criminal Prosecution (Bundeskriminalamt-BKA) has voluntarily passed guiding principles for police to follow in matching any data bases:

> The matching of entire data banks or important parts thereof with data banks that are not maintained by federal or state police, may only be conducted when the legal prerequisites in the individual case have been complied with and sufficient factual clues warrant its acceptance that this is necessary for the solution or prevention of complicated crimes, for the capture and arrest of wanted persons or for averting a present and serious danger in an individual case. A data match for the purposes of prosecuting crimes requires the prior approval of the Department of Public Prosecution [Staatsanwaltschaft].[24]

The guidelines further prevent direct storage or retention of the information obtained from such a computer match. They do not, of course, have the force of law and only apply to the BKA, an agency with jurisdiction similar to that of the FBI.

The West German bureaucracy has developed a widely-used though vague practice, known as interagency assistance (Amtshilfe). The practice is codified in section 68 of Book Ten of the Social Code. Under the guise of this principle, an agency can provide to another agency information consisting of the given name and surname, date of birth, place of birth, the current address, and the name and address of the current employer of an individual, "as long as there is no reason to assume that the interests worthy of protection of the person concerned will be infringed thereby."[25] Although this practice broadens record-linkages within the boundaries of the five types of information that may be provided, Professor Bull believes that interagency assistance means only assistance in the individual case and that large-scale procedures such as computer matching cannot be carried out solely on the basis of this provision.[26]

Furthermore, interagency assistance is secondary to other sources of information, and section 68 provides that the agency from which the information is sought is not bound to release the information, "when the agency seeking the information can obtain the data in another manner."

The BKA has developed a form of information searching which is essentially a pattern-search recognition technique (Rasterfahndung). In late 1979 and early 1980 the BKA used this technique to find a suspected terrorist in Hamburg, who was known by name. The police knew from experience that terrorists often rented apartments and had the electricity bill for that apartment charged in the name of the landlord;they then reimbursed the landlord. The BKA accessed the billing records of the Hamburg Electricity

Board to discover the names and addresses of persons who had unusually large consumption rates for their homes on the assumption that such persons might be paying the bill for the suspected terrorist. (They did not match the names obtained from the hydro records to the terrorist data banks, because they did not suspect the landlord of being a terrorist). By process of elimination, the police narrowed the field down to two thousand suspects who were interrogated and the terrorist discovered.

In a conference held in February of 1980 the federal and state data protection commissioners agreed that the Rasterfahndung technique was not contrary to data protection regulations and provisions and that section 24 of the Federal Data Protection Act, dealing with the permissibility of the dissemination of personal data by private bodies in the interests of the general public, permitted this practice.

Computer matching is also a problem at the state level in West Germany, since the state governments are also trying to reduce the costs of social security and have created various computer profiles of individuals in order to do so. Such profiles can lead to administrative action against specific persons. In Hesse, the data protection authorities are anxious not to appear as being totally hostile to computer matching. They are trying to figure out a way to resist the practice without being labelled as Luddites. The administrative authorities in the states of North Rhine-Westphalia have used computer matching to produce examples of physicians engaged in illegal billings. In these types of examples, the problem of controlling computer matching is framed in a fashion that is very similar to the current federal situation in the United States. The general problem is the attempt by governmental authorities to use personal data in new ways to try to reduce the costs of government programs.

Another form of record linkage is the creation of a personality profile on the individual. Unlike the French data protection law, West Germany's Federal Data Protection Act does not expressly prohibit creating a personality profile or basing a decision on human behaviour solely on a computer file which defines the profile or personality of the person concerned.

The police authorities in the Federal Republic are able to create a form of personality profile by linking information from several of their own data bases. The federal BKA is linked to the police at the state level through a system known as INPOL. The BKA also runs a system known as PIOS. This system gathers information on people, housing, and terrorist activities, including details of membership in associations, the use of domestic utilities, car rentals, library use and books read, and the frequency of phone calls.[27] A recent report by France's Agence de l'informatique states that "every file included in PIOS and INPOL can be connected and mixed to others for research process, so that a single [piece of] information is enough to draw a complete picture of a suspected person."[28]

The issue of producing computer profiles is particularly framed in West Germany by the development of personnel information systems. Data protectors suggest that these systems produce an illusion of rationality in data processing. Labour unions are very sensitive to this issue as well and opposed to it. They see personnel information systems as a form of control of employees by paying detailed attention to such matters as absences from work, illnesses, lateness, and food and alcoholic intake.

Certain data protectors in West Germany regard personnel information systems as destroying the balance of power between employers and employees. Such a point of view indicates the expansive thinking of some data protectors on certain subjects. One of the principles pursued by federal data protectors is to expect the elected representatives of employees in a particular concern to give informed consent to data collection. When the federal data protection office inspects a particular personnel system, they ask for a list of all the contents of the individual files and all uses and linkages of personal data. Data protectors question certain practices and, in particular, are strongly in favour of the erasure of personal information after a specific time period. They are especially keen to limit the collection and storage of sensitive personal information. Because of the highly legalistic character of data collection in West Germany, data protectors also demand that a legal basis should exist for the collection of specific personal information. This is also a requirement of the major decision of the Federal Constitutional Decision in December 1983. Data protectors are also in a position to debate the need for specific items of information with employers who are doing the data collection. Such issues arise at both the federal and state level in West Germany.

3.6 Australia

The recent report on privacy of the Australian Law Reform Commission contains some very useful material about computer matching by the federal government, including concrete examples of the matching practices in the fields of health, social security, and taxation. Since these data are very well organized and presented in this document, they are not summarized here.[29] Moreover, the analysis and level of awareness of the problems posed for privacy by matching are very similar to the preceding pages of this report. In the Commission's view, "it cannot be assumed that matching techniques in themselves pose an unreasonable threat to privacy. Matching may, or may not, provide an incentive to provide honest information on which sound judgments can then be made by the collector. But even where matching has just such a legitimate function, it should not be implemented without proper consideration of privacy implications."[30] In Australia, the proposed Privacy Commissioner would be involved in such a process. The Commission also recognized the pressures promoting matching: it "can play a significant part in containing the cost of government operations, reducing fraud and other abuses of the revenue.... There is a legitimate interest--a public interest--in ensuring that public money is not overpaid or mispaid. Matching is one way of ensuring that this does not occur."[31]

The Law Reform Commission concluded that "the same principles should apply to the use of matching techniques as apply generally to the use and disclosure of personal information." It recommended that those considering, designing, and operating any particular match should, in addition to seeking legal authorization, consider the following matters:

1. The dangers of comparing information collected for one purpose with information collected for another purpose.
2. The possible inconsistency of information, produced by the differences between the contents and times of the collections; and
3. Whether an opportunity is to be afforded for full explanation of apparent discrepancies before any action is taken prejudicial to an individual.[32]

Notes

1. See Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs. Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, 97th Congress, 2nd Session, Dec. 15-16, 1982 (Washington, D.C. Government Printing Office, 1983). [Hereafter cited as Oversight of Computer Matching.]

2. See Privacy Commissioner of Canada, Annual Report, 1983-84 (Ottawa: Ministry of Supply and Services, 1984), pp. 3-4.

3. Record linkages are a standard practice of national statistical agencies, especially for such purposes as the conduct of epidemiological research. Although such linkages are indeed often sensitive and controversial, the focus of discussion in this report is record linkages for administrative purposes. I have discussed research linkages in David H. Flaherty, Privacy and Government Data Banks. An International Perspective (London: Mansell, 1979), especially the index entry for the topic.

4. Oversight of Computer Matching, pp. 1-2.

5. Ibid., p. 473.

6. See the discussion in ibid., pp. 480-86.

7. Privacy Commissioner, Annual Report, 1983-84, p. 3.

8. Ibid., p. 4.

9. Ibid., p. 4. This report, including the warnings about computer matching, attracted widespread newspaper coverage. See The Globe and Mail, July 5, 1984, pp. 1-2; The Toronto Star, July 5, 1984, p. A3.

10. See Marina Strauss, "Delinquent spouses face opening of private records," The Globe and Mail, July 27, 1983, pp. 1-2; "The new alimony diversion project," Maclean's, April 23, 1984, pp. 46-7; and Jeff Sallot, "Aid Coming on

Alimony: Crosbie,"The Globe and Mail, November 24, 1984, p. 1.

11. Jeff Sallot, "Voters' list used in hunt by taxmen," The Globe and Mail, Nov. 1, 1984, pp. 1-2.

12. B. K. Dertinger, "Computer Matching and Linking of Personal Information in the CEIC," Science Council of Canada, Workshop on Information Technologies and Personal Privacy in Canada, Ottawa, Oct. 1-2, 1984; and Jeff Sallot, "Computer sleuthing leads Ottawa to millions in jobless overpayments," The Globe and Mail, Oct. 3, 1984, pp. 1, 4.

13. Dertinger, "Computer Matching and Linking of Personal Information," p. 3.

14. London Free Press, Oct. 6, 1984, p. A10.

15. Jan Freese, "Freedom of Information and Privacy Protection in Sweden," in Pierre Trudel, editor, Accès à l'Information et Protection des Renseignements Personnels (Montreal: Les Presses de l'Université de Montréal, 1984), p. 16. One of the ironic traits of Swedish data protection is that the DIB also promoted the creation of one single data bank of names and addresses (SPAR) for the public and private sectors, the use of which is governed by sections 26 to 28 of the Data Act. Its goal was to prevent the creation of even more national data banks.

16. Ibid., pp. 22-23.

17. Data Protection Act, 1984, s. 38(1); and Bryan Niblett, Data Protection Act 1984 (London: Oyez Longman, 1984), p. 87.

18. Data Protection Act, sched 1, Part 1.

19. Niblett, Data Protection Act 1984, p. 10.

20. Hans Peter Bull, Datenschutz oder die Angst vor dem Computer [Data Protection or Fear of the Computer], (Munich: R. Piper GmbHt, 1984), p. 284. Available in German only. [Bull wrote this book after the end of his five-year term as Federal Data Protection Commissioner.]

21. Ibid., p. 285.

22. Section 10, paragraph 1, numbers 7, 9 and 10 respectively of the (federal) Aliens' Act (Ausländergesetz).

23. Bull, Datenschutz, p. 286.

24. Ibid., p. 244.

25. S. 68, (federal) Social Code, Book Ten (of the Sozialgesetzbuch-X).

26. Bull, Datenschutz, p. 288.

27. Agence de l'Informatique. Personal Profiles and Automated Decision-Making. "Data Security and Confidentiality." A joint research program between ADI, GMD and NCC sponsored by the Commission for the European Communities and National Governments. (Draft Final Report). (Paris: January, 1983), p. 68.

28. Ibid., p. 69.

29. The practice and treatment of computer matching in Australia can be followed in paragraphs 88, 282, 292-93, 372-80, 409-11, 430, and 1321-24 of The Law Reform Commission, Privacy. Vol. 1: Background and Vol. 2: Proposals. Report No. 22. 3 vols. (Canberra: Australian Government Publishing Service, 1983). There is also a brief discussion of computer profiling in ibid., paras. 516, 543.

30. Ibid., Vol. 1, para. 282.

31. Ibid., Vol. 2, para. 1323.

32. Ibid., Vol. 2, para. 1423.

4. Personal Identification Numbers

The phrase, Personal Identification Numbers (PIN), is a generic reference to a whole series of numerical identifiers. An ideal PIN is a unique number assigned at birth that follows a person through life and is widely used in society for all administrative purposes. As noted in the discussion of record linkages in the previous chapter, few Western countries have truly unique numbers that are in common use for each citizen. Of the countries treated in detail in this research report, only Sweden has a PIN system that is mature and fully developed.[1] The other countries have numbering systems with varying kinds of problems, comparable to the unreliability of the Social Security Number in the U. S. as a unique personal identifier. Persons born in Canada have a unique number attached to their birth certificates, but it is not in common use; nevetheless, Canadians complain and worry about the use of their Social Insurance Numbers (SIN), which are the equivalents of Social Security Numbers. These numbers are the most common topic of complaints to the Privacy Commissioner, although there is little that this official can do himself about the issue, except for the potentially significant step of recommending to the federal government that it do something to control unauthorized uses of the SIN by federal and provincial governments and the private sector.[2]

Admittedly, persons worry about Social Security Numbers, Social Insurance Numbers, and other national identifiers, as if they really were unique PINs, and the numbers are in fact used as such, and as a linkage device, for most purposes. It is perhaps only specialists who wish to distinguish between reliable and unreliable PINs. North Americans are left with the semblance of a PIN system, with attendant problems of public resistance and paranoia, without any of the benefits for such purposes as epidemiological research, the inability to link health records over time, because of the absence of unique personal identifiers, is a significant barrier to better research on exposure to carcinogenic substances.

It is somewhat surprising that data protection laws do not specifically address the issue of PINs or other numbering schemes in use in the society; as a general rule the laws are silent on the problem, in part because most countries do not have single unique personal identifiers. In Canada, for example, the SIN is a source of continued anxieties, but it is not mentioned in the Privacy Act. The U.K. Data Protection Act 1984 does not mention the National Health Service number. Unique personal identifiers are not discussed in the basic text of the OECD Guidelines or the Council of Europe Convention.[5] The Swedish Data Act does not mentions PINs, which means that the use of the numbers is simply regulated like any other item of identifiable personal information.

The main point about PINs, whether unique identifiers or not, is that they are subject to strong resistance in Western Europe and North America, because persons believe that they threaten the very roots of personal privacy and individuality.

4.1 Sweden

The Swedish system of PINs ensures that the Data Inspection Board is particularly sensitive to issues of record linkages, because the PIN makes computer matching relatively easy. In fact, matching records without a PIN is not really practical or effective in any country, except for statistical purposes.

The DIB continues to receive complaints from individuals about the use of the PINs. The number is always being adapted for new uses, such as a recent introduction of an encoded PIN on a magnetic band on a particular person's drivers license (along with the existing photo of the holder). This occurred as all Swedish licenses, which are good for ten years, were being renewed. The motor vehicle bureau claims that the government had approved the practice, which was certainly not cleared with the DIB in advance. The latter was holding its fire on this particular point, until the Riksdag had finished its work on this specific measure. It is often acutely important for the DIB to know when to intervene in the case of a new application for information technology in order to be effective. It has to recognize that the use of the PIN is already pervasive in important and expensive systems in the private sector as well. Bank cheques have the PIN printed on them, for example. At the same time, the DIB realize that it will only be a matter of time before someone dreams up new uses for the PINs on licenses.

Although Scandinavians seem to have adapted to the existence of unique numbers, a Conservative Prime Minister of Sweden wanted to abolish the PIN in 1977. A typical study commission recommended its retention in 1978.[3] More recently, in early 1984, a leader of the Moderate Party gave a speech about the need to reduce the use of the PIN; this was part of his party's call for more freedom in Swedish society. The speech led to renewed media attention to PINs and illustrates how politicians searching for an issue regularly intervene on one side or another of the privacy debate in the various countries.

The Personal Identification Number remains a partisan political issue in Sweden. In what was effectively a way to postpone decision-making until after the national elections on September 19, 1985, the government recently appointed a study commission on the uses of the PIN and the possibility of restricting such uses. It will be expected to make concrete proposals within two years. The DIB is represented on the Commission by its deputy-director, Nils Ryden. Realistically, there seems little likelihood that the use of the PIN will be cut back significantly in Swedish society, because of the extraordinary costs that would be entailed. It is possible that the PIN Commission may try to curtail certain private sector uses of the PIN, such as on credit cards.

4.2 Federal Republic of Germany

In the 1970s West Germans resisted efforts to introduce a Federal Population Registration Bill that would include the introduction of a twelve-digit PIN for each inhabitant.[4] There were some suggestions that that government wanted to link the introduction of data protection and population registration, but the former preceded the other by three years. Critics argued that PINs were a fundamental threat to the principle of privacy incorporated in the constitution. Parliamentarians agreed in the early seventies that no system of data processing based on a unique personal identifier should be created without a corresponding system of data protection.[5]

The December 1983 decision on data protection of the Federal Constitutional Court will further impede the development of unique PINs in West Germany, since the court made negative comments about PINs in discussing the possibilities of carrying out a census of the population solely on the basis of administrative data bases (as is done in Denmark). The Karlshuhe court suggested that such a form of census would require PINs, which it described as even harder on the people than the present format for taking a census.

The current system of numeration system is one in which separate government agencies develop and use their own numbering systems for particular purposes. For example, West Germany currently has a pension insurance number

(Rentenversicherungsnummer) for use in the social insurance system, but this number is not used as a general personal identifier, unlike the Social Security Number in the United States.[6]

In the summer of 1980 the Bundestag passed the Registration Act (Melderechtsrahmengesetz), dealing with population registration; it does not include provisions for PINs. The duties of the registration authorities, as set out in section 1, are "to register the inhabitants in their area of jurisdiction in order to be able to establish and prove their identities and places of residence." Section 2, paragraph 2, also permits the registration offices to use their information in preparing for elections, issuing income tax cards, personal identification cards, and passports, and to assist in military and civilian service surveillance. To fulfill these duties, the population registers are permitted, by paragraph 1 of section 2, to share nineteen types of data including given name and surname, address, date and place of birth, religious affiliation of the indivdual and of his spouse, citizenship, date of entry into the country, principal and additional residence, family status, income bracket, tax exempt allowances, legal status, relation to children, and address of foster parents and stepparents. States, through their own laws, can expand the list of the information permitted to be stored (section 2, par.3). The principle of necessity to fulfill legal tasks governs what information is to be released to an agency.[7]

4.3 France

Article 18 of the French data protection law of January 6, 1978 stipulates that "use of the national identification register of natural persons [RNIPP] with a view to processing of personal data may be authorised by order of the Conseil d'Etat after advice from the Commission." This RNIPP contains a set of what might be described as national identification numbers for about fifty million individuals. This type of national population register is maintained by the national statistical agency, the National Institute of Statistics and Economic Studies (INSEE). The numbers assigned to all newborn children are in effect Personal Identification Numbers, which are used for a limited number of other purposes such as social security and the electoral register.

The CNIL initially investigated the RNIPP and issued a favorable decision on its existence on January 22, 1982. All specific uses of the RNIPP have to be approved in detail by the CNIL, which determined that in general it should not be used to search for persons, unless directly authorized by law. Only very restricted personal information can be kept in the RNIPP, including names, dates and places of birth, and the national identification number.

Thus, as in the case of any other use of personal data by a government agency, the National Commission on Informatics and Freedoms (CNIL) has to review and advise on a proposed use of the RNIPP, which it is doing on a case by case basis. On June 25, 1984, for example, the CNIL authorized the Compatibilitē Publique, a government financial agency, to use the RNIPP to pay state pensions, because no other efficient method was available to reach the same result. In general, the CNIL restricts uses of the data base but allows it to be consulted for other purposes, such as verifying the existence of a person. The ultimate need for the Conseil d'Etat to make the final decision on applications of the RNIPP is some indication that such data uses are sensitive. The CNIL will have to be vigilant to prevent expanding uses for the RNIPP data base and the national identification numbers themselves. Their use for purposes of tax collection has not yet been regulated.

[no page 73]

Notes

1. The Swedish ten-digit PIN system is discussed in David H. Flaherty, Privacy and Government Data Banks. An International Perspective (London: Mansell, 1979), pp. 101, 115-16, 117-18.

2. The only research report carried out by the first Canadian Privacy Commissioner, Inger Hansen, Q.C., was on the SIN. See Report of the Privacy Commissioner on the Use of the Social Insurance Number (Ottawa, 1981). The first speech of Dr. John W. Grace as Privacy Commissioner (on Sept. 22, 1983) was on the SIN. I argue that the new Progressive Conservative government of Prime Minister Mulroney should take visible steps to restrict unauthorized uses of the SINs, because public concern on this specific issue remains so high, and the Conservatives in Opposition made such a continued fuss on the matter. See The Globe and Mail, December 19, 1984, p. 6; and David H. Flaherty, The Origins and Development of Social Insurance Numbers in Canada (Ottawa: Department of Justice and Privacy Commissioner, 1981). SINs were created in the early 1960s for specific purposes of administering federal government programs in the tax, old age pensions, and unemployment insurance fields, but no one was wise enough to forbid their use for other purposes; inevitably, such uses have multiplied to where the SIN is used *de facto* as a PIN.

3. Flaherty, Privacy and Government Data Banks, p. 101.

4. *Ibid.*, p. 162.

5. Hans Peter Bull, Datenschutz oder Die Angst vor dem Computer (Munich: R. Piper, 1984), pp. 195-96.

6. *Ibid*,, p. 195 and, in general, pp. 190-98.

7. *Ibid.*, p. 200

5. Machine-Readable Identity Cards and "Smart" Cards

One is tempted to analyze the debates over machine-readable identity cards and other forms of "smart" cards as simply a classic example of a new technology looking for an application, promoted especially by the private sector and, typically, regarded as a "fix" for a particular problem by the public servants involved. The identity cards in question essentially involve a traditional plastic credit card impregnated with selected amounts of personal data, which a machine can scan very quickly in order to validate a transaction such as crossing a national boundary. The latter is the most commonly discussed application of the cards at present, but what is inevitable is that new applications will be invented as fast as machine-readable cards can be dispensed; thus they do pose a significant challenge to the individual interests that data protectors are trying to protect through the application of their general laws in specialized laws or regulations.

5.1 Federal Republic of Germany

On November 1, 1984 the German government had planned to introduce machine-readable identity cards for the control of persons crossing frontiers. The motivations included improved efficiency at airports and creating a card that was very difficult to counterfeit, because it would be issued by only one agency. Data protectors insisted on rules in the relevant law of March 15, 1983 about how the cards could be used solely for border crossings, but there were intelligent concerns about whether such controls on multiple uses would be effective in the long run. Because of the census controversy in 1983 and the decision of the Federal Constitutional Court, the introduction of automated cards has been postponed. Data protectors plan to use this opportunity to seek stronger provisions for data protection in the special legislation that controls any such measures in West Germany.

The Personal Identification Act (Personalausweisgesetz) in its current form already contains provisions which conform to data protection principles. More particularly, the Act specifies what information can be contained in the card; it prohibits the inclusion of a fingerprint; the serial number on the card may contain no information on the individual; no central data base of all card-carriers may be established other than for the immediate purpose of printing the cards; the serial number may not be used to correct or link data bases; the cards may only be read by machines for the purposes of border control, searching for persons and investigating crimes by the competent authorities; and the use of the serial number by the private sector is prohibited for the purposes of establishing or linking data bases.[1]

It is worth noting that the existing system for border controls involves a process of photographing the passport at the entry point, leading to an immediate check of its legitimacy by a secretary using an on-line system. Thus the use of an automated identity card for similar purposes would involve only marginal changes, except for the possibility, well recognized by the data protection authorities, that new uses for such a device are bound to spring up and to be difficult to control. However, only a very small percentage of the more than 800 million border crossings each year are being checked at present, and President Mitterand and Chancellor Kohl announced in 1984 that border checks between their two countries would cease.

Thus the situation with respect to the introduction of automated identity cards is very much in flux at present. Data protectors regard the issue as a difficult one. They are asking the government to explain the current need for a new automated card, especially because of the risks of the development of multiple uses and the storage of data to produce profiles of individuals. One possible solution is to allow a new form of identity cards without automation, since cards of this type already exist. At this point, the issue is also very political. The Green party does not want any identification cards, the Social Democrats are opposed to automated cards, while the Coalition government accepted them.

5.2 Canada

In Canada it is reported that the Department of External Affairs wishes to introduce machine-readable passports, presumably in imitation of similar American and British practices and plans, but no significant public debate has occured on the implications of such cards has occurred. The London Free Press did make the intelligent editorial comment that: "There is nothing wrong with a new passport that will improve airport processing; there is a problem, however, with the type and amount of information to be stored in the data banks for matching against the passport carrier."[2] The fundamental point is that automated passports or identity cards, whatever their other merits, have certain implications for the privacy of individuals, which need to be studied and evaluated in detail by specialists in data protection. Canada and the U.K. are fortunate to have date protection officials in place who can be involved in this process on a consultative basis.

5.3 Sweden

"Smart cards" have not been much of an issue for data protectors in Sweden to this point in time, although any new form of information technology, involving personal information, eventually has to come before the Data Inspection Board for a license or, sometimes, explicit permission. For example, Scandinavian Airline Systems (SAS) has some plans to use smart cards for reservation purposes, whereby an individual will not receive tickets for a trip but a number and code for the smart card. The SAS computer system can then interact with the card to store all kinds of information concerning a person's particular reservations. Although travellers can envision some advantages to such a system, residents of Sweden have the benefit of knowing that the privacy implications of such an innovation will have to be considered in advance of implementation rather than, as is so often the case in other countries, as an afterthought to an entrepreneurial concept.[3]

5.4 France

On December 25, 1979 the French Ministry of the Interior announced plans to produce and distribute a new form of national identity card that would be manufactured by computer and encased in plastic. It had all of the characteristics of a credit card, including magnetic stripes and thus could be made machine-readable and linked to other information systems. In 1980 the introduction of these cards became controversial in the press and with trade unions.

The CNIL's positive decision on the new national identity cards was eagerly awaited. It forbade the inclusion of existing social security numbers, or any other unique numbering system for individuals on the cards. The French government moved forward with the manufacture of the cards in the summer and fall of 1980, managing in the first instance to produce cards without the proper accents on the names of individuals.

The election of the Socialist government was the salvation of the opponents of automated identity cards, since it regarded them as a real danger to individual liberties and private life. On September 12, 1981 the new Minister of the Interior's announcement ended the process of issuance of cards.

It is arguable that the new government's decision casts a relatively harsh light on the prior decision of the CNIL, which in effect assured the population that automated identity cards did not challenge the values protected by the data protection law of January 6, 1978.

Automated identity cards are not yet a dead issue in France, especially since fraudulent identity cards remain a problem. One of the promised benefits of automated cards in several countries is reducing the prospect of counterfeiting them. The CNIL receives continuing proposals from the Paris police in particular to find ways of preventing individuals from receiving multiple identity cards. It approved an automated system of checking for fraud on January 17, 1984, after receiving assurances about the extent of security safeguards in the computer system of the Paris police. The system crosschecks for different applications for identity cards to the twenty different bureaus in Paris that issue them. At the end of 1984 the CNIL determined that the Bureau of social assistance in Paris could not require applicants to furnish two copies of their identity cards in order to prevent the use of fraudulent cards. Thus the experience with a general plan for automated cards has seemingly made the CNIL more sensitive today to their implications for privacy.

Among European and North American countries, France is the most advanced with respect to the development and application of what are called cartes à mémoire or cards with a memory (smart cards). The idea of inserting an electronic device in a plastic card was invented by a Frenchman, Roland Moreno, in 1974. The technology is being developed and implemented quickly, since competition from the Japanese is feared. The cards can already store eight kilobits of information and soon are expected to reach sixteen kilobits.

The French distinguish three levels of smart cards from the simple memory cards to cards with a microprocessor. The former are passive and cheap to produce; they are used to operate toll phone booths and purchase units in stores. An example would be a smart card "charged" with a fixed amount of money that can be spent until exhausted and then replenished. The second level of card (cartes à logique cablée) contains a logic system which controls access by a reading device to the information stored in its memory. This card cannot be reprogrammed, so uses and purposes have to be specified in advance. The highest level card contains a microprocessor, can be programmed for new applications, and can have a high level of security. The cards introduced by CII-Honeywell Bull and Philips use this approach.

A variety of experimental and operational uses of smart cards have been introduced, since the French telephone and postal authorities (PTT), financial houses and banks created the GIE Carte à Mémoire Group in March 1980.[4] Three different companies have been testing 100,000 payment cards and 600 terminals since the fall of 1982 in Blois, Caen, and Lyon. The Ministry of Social Affairs has been introducing 10,000 "personal health cards" in Blois since 1984 on a two-year experimental basis. They are portable data banks in which new information can be entered. An authorized physician can read the card, insert new information, and alter existing data by means of a special authorization card. The Bull company has introduced such cards for dialysis patients. More applications are being developed and introduced on a continuing basis.

Like any other new form of technology involving the use of personal information, applications of smart cards in both the public and private sectors are subject to various types of regulation by the CNIL. The system in place is to rule on each application on a case by case basis. For example, on

February 21, 1984 the members of the Commission heard a presentation about the privacy implications of an experiment with smart cards for the educational records of 8,000 students at the University of Paris VII. The evaluation and subsequent approval by the CNIL included a fifteen-page report on the project. It tends to regard this type of intelligent card as a portable data bank, which the owner can control through the use of access codes. The argument appears to be that this may be the ultimate data bank for insuring informed consent by the individual.

At the annual international meeting of Data Protection Commissioners held in Vienna in September 1984, members of the CNIL made an oral and written presentation about smart cards. In their judgment, smart cards offer improved levels of security to control unauthorized access. They recognize certain potential access problems, if the holder of a smart card for medical purposes cannot in fact read certain items of data in his portable file. In a manner typical of expansive French data protectors, the CNIL also expressed their concern at Vienna that the introduction of this new form of technology might marginalize sectors of the population who cannot afford payment cards or cards to activate telephones.

Notes

1. Federal Data Protection Commissioner (Der Bundesbeauftragte für den Datenschutz), Sechster Tätagkeitsberticht des Bundesbeauftragten für den Datenschutz (Sixth Activity Report of the Federal Commissioner for Data Protection). (Bonn: Bonner Universitäts-Buchdruckerei, 1983), p. 6.

2. See London Free Press, Oct. 6, 1984, p. A10.

3. To the best of my knowledge, there are no current plans to introduce machine-readable identity cards in Sweden.

4. Details in this and the preceding paragraphs are from a looseleaf publication by Groupement Carte à Mémoire, Les spécifications et les normes de la carte à mémoire bancaire (Paris, France, 2nd edition, September, 1984).

6. Conclusions

This report for the Office of Technology Assessment has had as its primary purpose the presentation of information and analysis about how privacy and data protection laws are functioning in western countries other than the United States. In addition, certain specific issues associated with new information technology, such as computer matching and profiling, Personal Identification Numbers, and machine-readable identity cards have been treated in more detail in terms of how data protection officials handle their implications for personal privacy.

The primary conclusion of this report, and of my ongoing research on "Data Protection in Comparative Perspective," is that the system of data protection in place for the public sector at the federal level in the United States is sorely lacking one key ingredient, and that is an effective oversight mechanism to ensure that the Privacy Act of 1974 is implemented in an appropriate fashion.

The lack of a federal data Protection Commission in the United States is a source of concern to foreign data protectors, since they believe that an agent or agency is an essential component of a data protection system, a perspective reinforced by the fact that all other national laws include an oversight mechanism. Moreover, the Europeans have no comparable agency in the United States to deal with, especially on the sensitive subject of transborder data flows of personal information. Finally, the American representation at the annual international meetings of Data Protection Commissioners is either non-existent or minimal, since those present from the United States government adopt a very low profile in such a setting, perhaps in part because the American system is so different, at least in structure.

One of the several practical reasons why the United States should consider setting up a national data protection agency is that the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) is about to acquire the force of law, permitting foreign countries to authorize unrestricted flows of personal information across their borders when other countries have designated authorities for data protection in place. It would seem at least somewhat difficult to persuade Europeans that they should not limit transborder data flows to the United States, since there is no Commission or Commissioner for them to deal with on data protection issues.[1]

My general inclination, as noted above, is to identify certain problems of the data protection movement, while being fundamentally committed to its general goals. As discussed further below, I am concerned about how effective data protection will be in the long run, as bureaucratic considerations and human inertia become more powerful influences than they have been during an exciting first decade for data protection on the international stage. But, in certain ways, this emphasis in my approach has certain benefits for the United States, since, at a time when the Privacy Act of 1974 certainly is in need of a general review, data are available to assess the data protection movement elsewhere in a critical fashion. No one should be led to believe that a Data Protection Commission in the United States would be a universal panacea and/or always succeed in resolving conflicts over values in the direction of promoting privacy. One of the lessons of the material presented above in chapters 2 to 5 is that data protection agencies are only one player on the political and legislative scene; nevertheless, it seems essential that this player be on the field when interests affecting privacy are under discussion.

Having already discussed my perception of the general need for an oversight mechanism and the fact that I judge the initiatives in data protection to have been generally effective, the remaining paragraphs will attempt a general, brief assessment of the strengths and weaknesses of data protection policies and practices to date in countries outside the United States.

A prime characteristic of data protection agencies to date is that they have been very resistant to their own bureaucratization. The largest national agencies in France, the Federal Republic of Germany, and Sweden have less than forty professional and clerical staff. Such leaders of the data protection movement as Jan Freese in Sweden and Professor Spiros Simitis in West Germany have been consciously and articulately opposed to the building up of large staffs. In fact, in the case of both of these persons, the argument can be made that their respective staffs are in fact too small for the legislative responsibilities that they face. Nevertheless, the general resistance to bureaucratization strikes a positive response in the 1980s.

As a general rule, the actual costs of creating and operating data protection agencies have been relatively modest, especially in terms of general government expenditures. No one has successfully accused any of these agencies of being too expensive. The internal process of controlling the costs of data protection has also been reinforced by the general restraint programs adopted by all Western governments in recent years. Like most efforts at cost assessment, it is difficult to know just how much complying with data protection has cost the various branches and agencies of any national government. One premise of the data protectors themselves is that reducing the amount of data collection and storage and requiring good security measures for personal information are beneficial, and in some respects cost-cutting, activities in themselves. In West Germany, for example, the staff of the federal data protection office are routinely consulted as specialists in efficient (and well-regulated) flows of personal information.

The prevailing sentiment in the data protection community outside the United States almost approaches the view that data protection is too important and too complicated to be left to the courts. The argument is that data protection in its application is a complicated and specialized business which courts are not equipped to handle on an ongoing, systematic basis. At the same time, there is no desire to interfere with the exercise by individuals of their traditional legal rights, or the use of the courts to handle criminal prosecutions under data protection laws (a rare occurrence to date in the several countries.)

The quality of the leadership and staff of any data protection agency is an essential ingredient in the recipe for success. Perhaps because of the novelty of the subject and its perceived contemporary importance, these relevant agencies have for the most part attracted very high quality leadership and staff. There are some concerns about how long this process will continue, as office practices and issues inevitably become more routinized. Some experienced data protectors have become firm believers in rotating both the leadership and staff members of an agency in order to promote the necessary enthusiasm for the conduct of a burdensome activity.

The issue also arises in connection with staffing of whether it is necessary or desirable for data protectors to be perceived (by their critics) as "fanatics" in pursuit of the statutory goals of data protection legislation of preventing unwarranted invasions of privacy. Given the tiny size of any data protection agency in comparison to public administrations and the large data processing community, it is arguable that data protectors have to be tenaciously dedicated to the goals of good data protection, since the tasks of effective implementation are so enormous in scope in all advanced industrial societies.

A related issue concerns the political realities of the exercise of power by a data protection agency. Experience to date in West Germany and Sweden illustrates the possibilities of successful action by strong leaders supported by a talented staff. At least in the first five years, the French have demonstrated less political will. This issue raises the general question of the extent to which any data protection agency can resist any government's desire to use automated personal information for any purpose. Despite the fine track record of most of the countries with extensive experience in data protection, the risks exist in any country of providing only the illusion of data protection, with data protectors in fact serving as agents of legitimation for new forms and uses of information technology. Of the three countries discussed so far in this report, which have significant experience with implementation, this risk is greater in France than elsewhere. The problem is essentially one that will require continuous monitoring by those interested in the protection of privacy.

Perhaps the great strength of data protection agencies is in providing a permanent source of expertise for the attempted resolution of issues and practices affecting the privacy interests of individuals in the several societies. Protecting privacy begins with problems of definition and moves inexorably towards difficulties in balancing competing values in an intelligent and rational fashion. The issues arise on and item by item basis, as the discussion above in chapters 2 to 5 suggests. The great value of a data protection agency is to seek to resolve specific data protection problems. The experience to date suggests that they are both qualified and competent to accomplish these tasks. The irony is that this same impulse leads to the accusation that data protectors may in fact function as legitimators of new information technology and new practices, such as record linkages. In my judgment, it is in the best interests of any society to have in place a mechanism that can review, modify, and ultimate accept, or at least tolerate, such activities.

Notes

1. Article 13 of the Convention only requires parties to designate one or more authorities to promote cooperation on transborder flows of personal data. The explanatory memorandum to the Convention underlines that "this does not mean that the convention requires each State to have a data protection authority." However, memorandum also anticipates that "many States may in practice wish to entrust mutual assistance in data protection matters to authorities specialised in this field. Most countries having a data protection law also have a special protection authority." See Council of Europe, Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg: Council of Europe, 1981), pp. 23, 34-5.

Research Note

The argument that a data protection agency (or agent) is essential for successful implementation of data protection laws is not an assumption on my part but a personal judgment. It is the major conclusion of an international research project on data protection, begun in 1981, involving considerable interviewing and empirical research in six countries that are the primary targets of my research, plus some direct exposure to the situation in Denmark and Norway. My research on data protection in countries outside North America began in 1974 and has remained reasonably intensive since that time. I am in the fortunate position of being among the very few privacy advocates that has been able to develop a reasonable understanding of the system and practice of data protection in more than one country. For example, I conducted regular interviews with U.S. federal agencies on the implementation of the Privacy Act.

Thus, my research on data protection has included the United States and is based on a reasonable understanding of the American constitutional, legal, and political systems, since, under another hat, I am an academic trained in American history with a particular emphasis on legal and constitutional history.[1] After graduate training at Columbia University, I taught general American history and legal history for seven years at Princeton University and the University of Virginia before returning to Canada.

I began my current research project on data protection in 1981 with an open mind about the need for a data protection agency in any national system. When I prepared invited testimony for the first oversight Hearings in June 1983 on the Privacy Act of 1974, I was clearly struck by the major structural deficiency in the American system, where the Office of Management and the Budget has not fulfilled any kind of continuing and meaningful oversight role since 1974, at least comparable to the accomplishments of counterpart data protection agencies in other countries.[2] I regard it as an unfortunate accident that the United States did not create a Privacy Protection Commission in 1974, as Senator Sam Ervin, Jr. and his colleagues attempted to do in the Senate version of the Privacy Act.

One of the accomplishments of the Bellagio Conference on privacy and data protection in April 1984 was to bring together specialists from nine countries, including the United States, for intensive discussions of their respective systems of data protection.[3] Those present acknowledged that there were substantial protections in place for personal privacy in the United States, and considerable progress was made in having key persons appreciate certain merits of the American system. Nevertheless, in my judgment, the rationale for the continuing failure to create a data protection agency in the United States was not apparent.

One of the problems of writing this current report for OTA has been that I am very supportive of the data protection initiative in the countries that I have studied, but I am also rather critical of certain aspects of its implementation to date in several countries. The identification of these problems, in the book on data protection that I am working on, is in fact an effort to contribute to the discussion about how data protection can be made even more effective than it has proven to be to date.[4] But it is one thing to be critical of the work of such agencies in an academic study that is designed to provide useful criticisms from the outside, but quite another to find oneself trying to study a system, such as the American federal one, which does not have an effective central focal point for data protection.[5] To the extent that there are deficiencies, in my view, in the national data protection schemes in place outside the United States, they are not structural in character.

Notes

1. My first book, which I began as a graduate student of Alan Westin's at Columbia University in September 1964, was a study of the concern for personal privacy that existed in early America. See Privacy in Colonial New England (University Press of Virginia, Charlottesville, 1972).

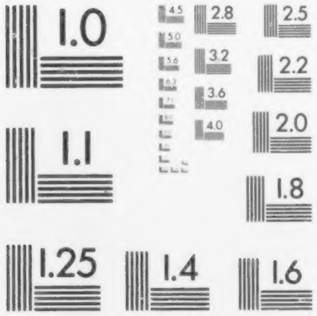
2. I have published a revised version of the June 1983 testimony as "The Need for an American Privacy Protection Commission," Government Information Quarterly, I, No. 3 (1984), 235-58. I would now prefer to have used the term "American Data Protection Commission," in order to avoid some of the political problems that arise from the breadth of the concept of personal privacy.

3. The report of the Bellagio Conference can be found in Government Information Quarterly, I, No. 4 (1984).

4. My judgment about effectiveness is drawn from empirical research, which I intend to elaborate on in detail in my prospective book on data protection in comparative perspective; it is not an assumption on my part, even though I do realize that it is difficult to measure "effectiveness" in implementation.

5. My judgment about the desirability of an effective mechanism in the United States to oversee the implementation of data protection is based on academic and structural considerations. I am not addressing the political realities of trying to create a Data Protection Commission in any country in 1984. For an informative discussion of the reasons why bureaucracies in two countries have resisted oversight mechanisms for data protection, see Priscilla M. Regan, "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations," Journal of Public Policy, IV (1984), 19-38.

MICROCOPY RESOLUTION TEST CHART
NBS - 1010a
(ANSI and ISO TEST CHART No. 2)



PHOTOGRAPHIC SCIENCES CORPORATION
770 BASKET ROAD
P.O. BOX 338
WEBSTER, NEW YORK 14580
(716) 265-1600

24:1

Congressional Information Service, Inc
Washington, D.C

CIS